FIG. 1

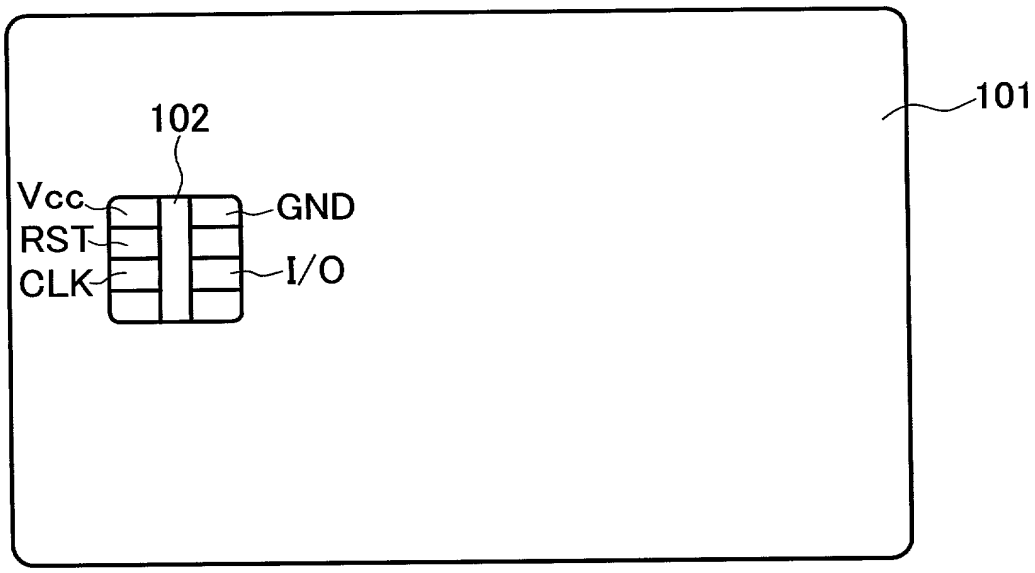


FIG. 2

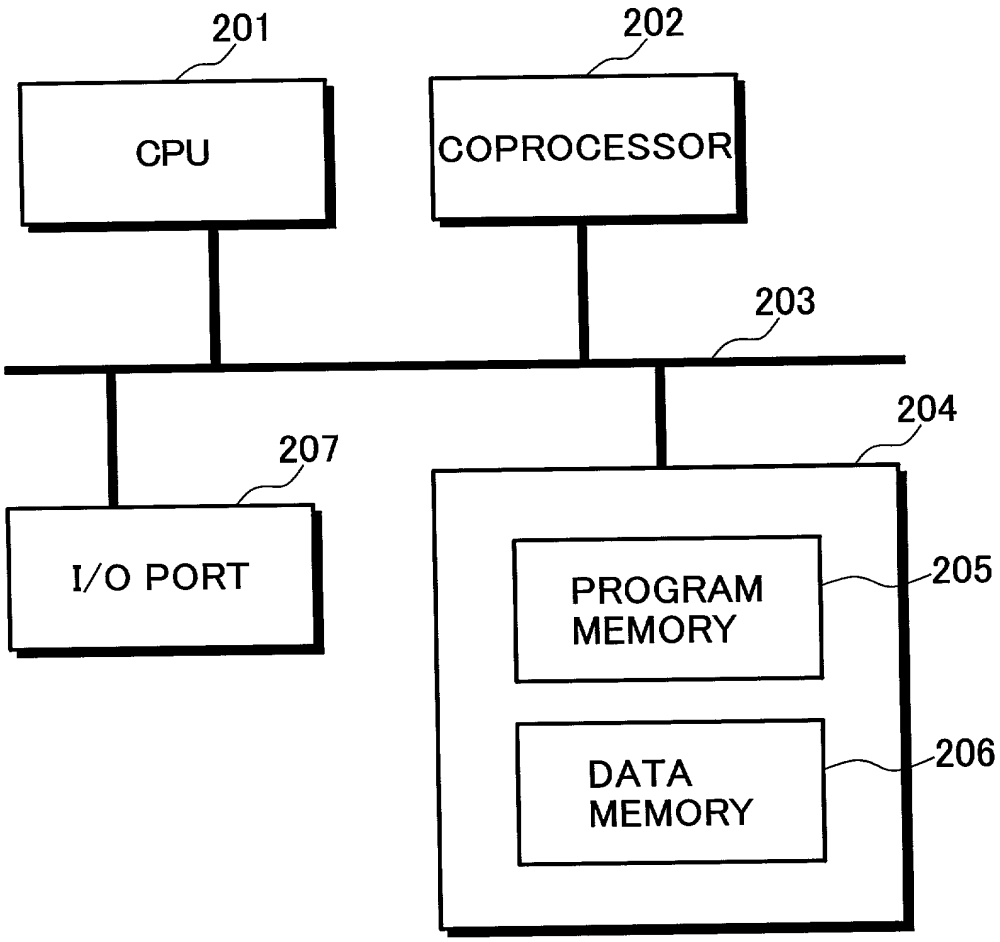

201
202
CPU
COPROCESSOR
203
204
207
I/O PORT
PROGRAM MEMORY
205
DATA MEMORY
206

FIG. 3

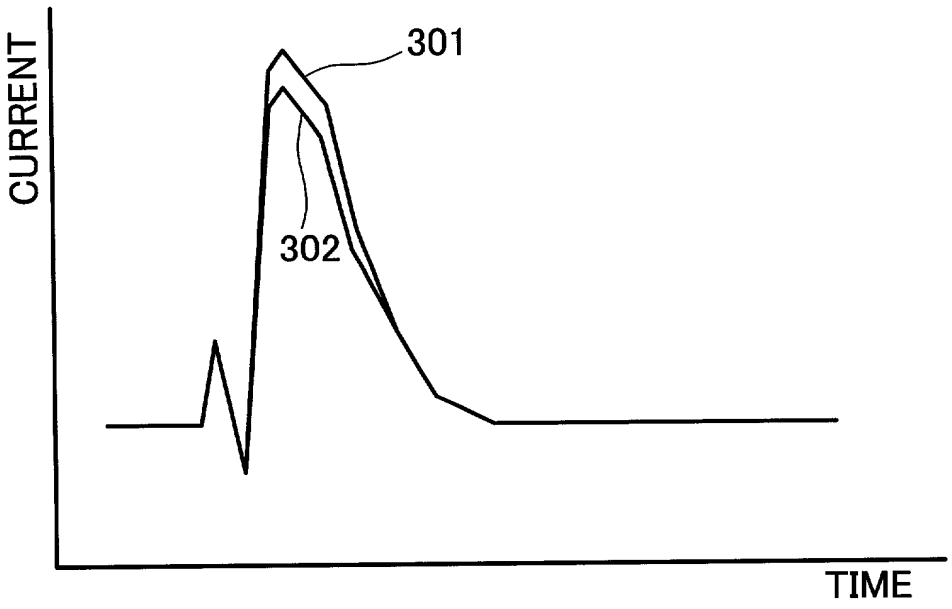
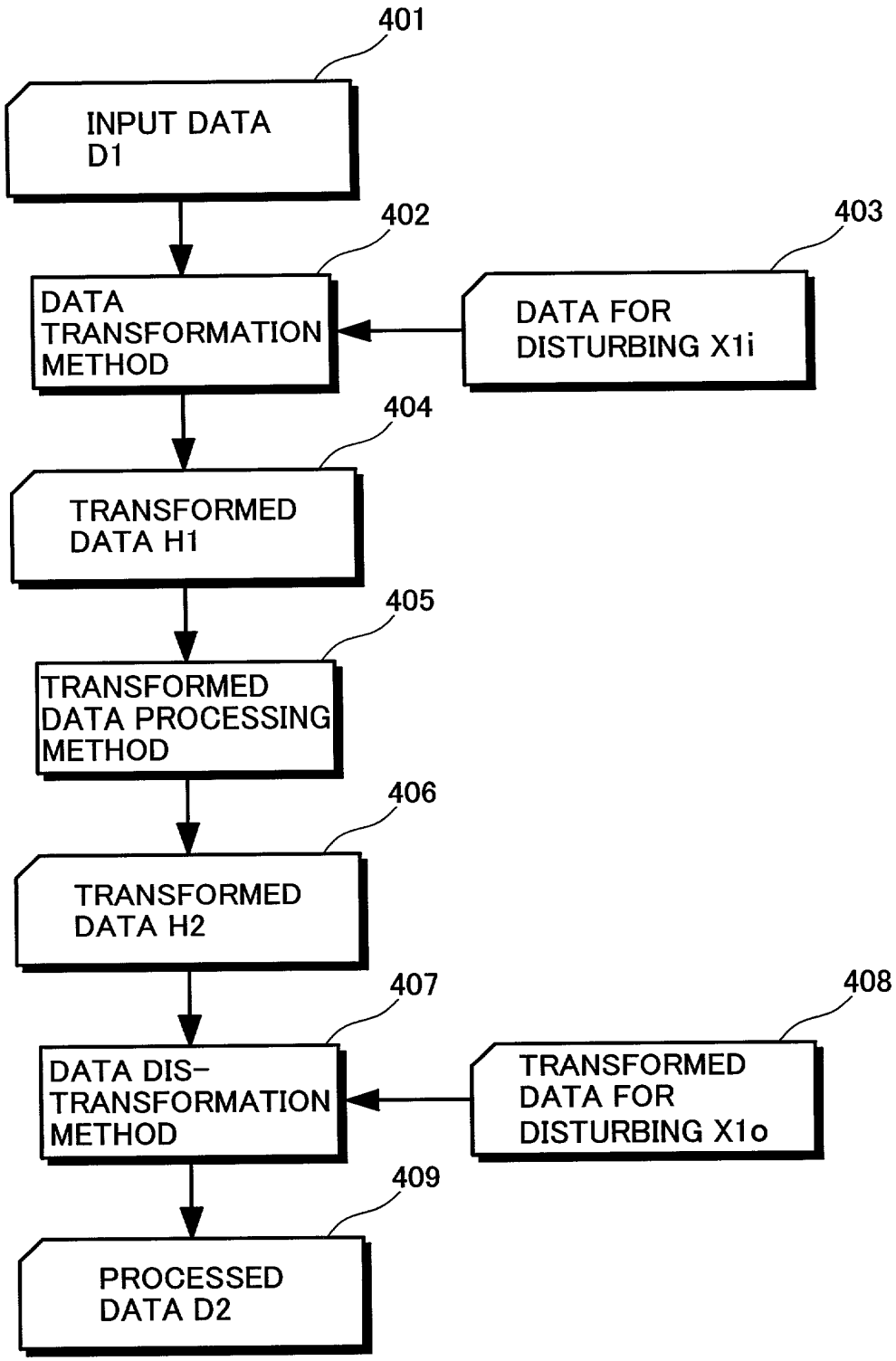


FIG. 4



JP 2005-062928 A 2005.03.10

FIG. 5

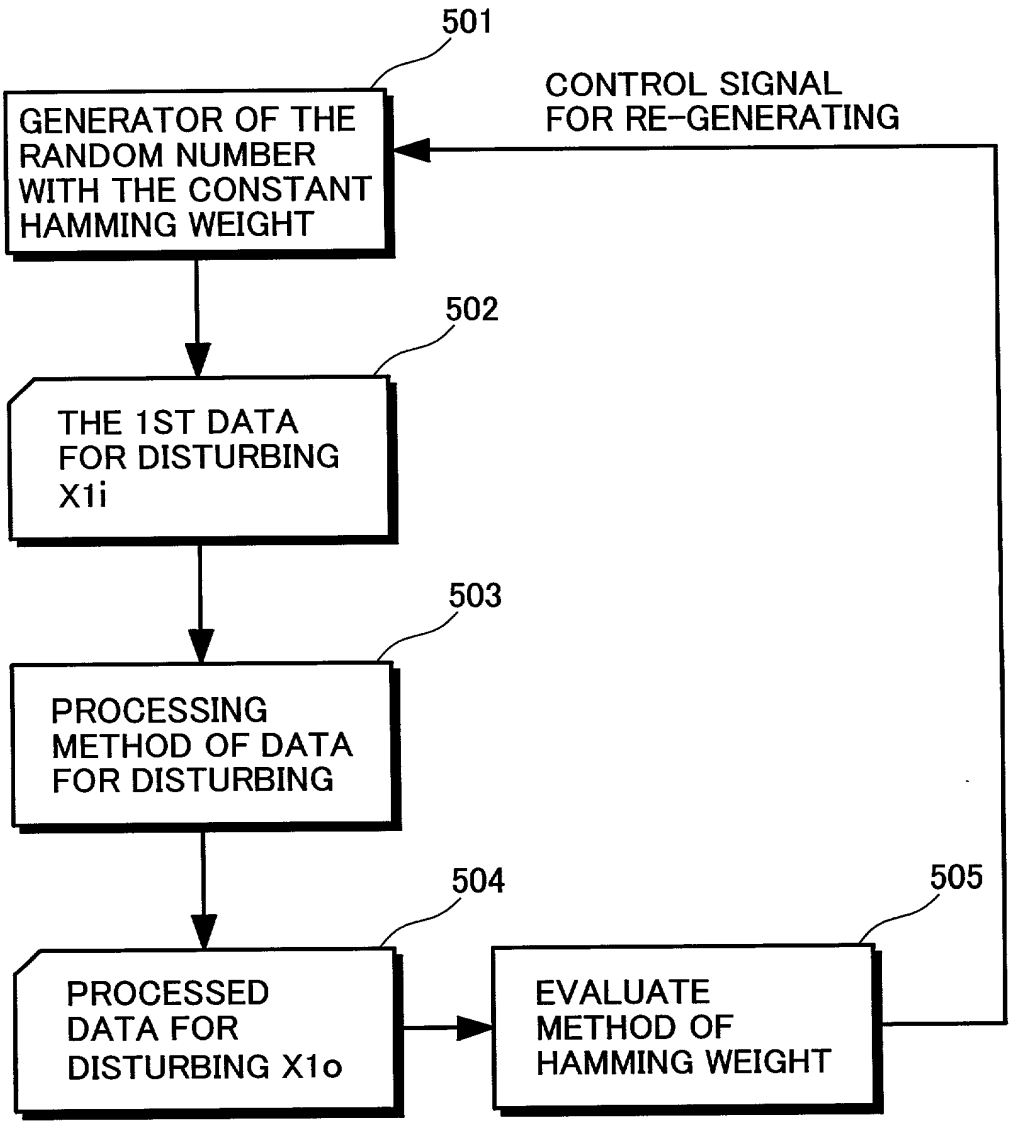

501
GENERATOR OF THE RANDOM NUMBER WITH THE CONSTANT HAMMING WEIGHT
CONTROL SIGNAL FOR RE-GENERATING
502
THE 1ST DATA FOR DISTURBING X1i
503
PROCESSING METHOD OF DATA FOR DISTURBING
504
PROCESSED DATA FOR DISTURBING X1o
505
EVALUATE METHOD OF HAMMING WEIGHT

FIG. 6

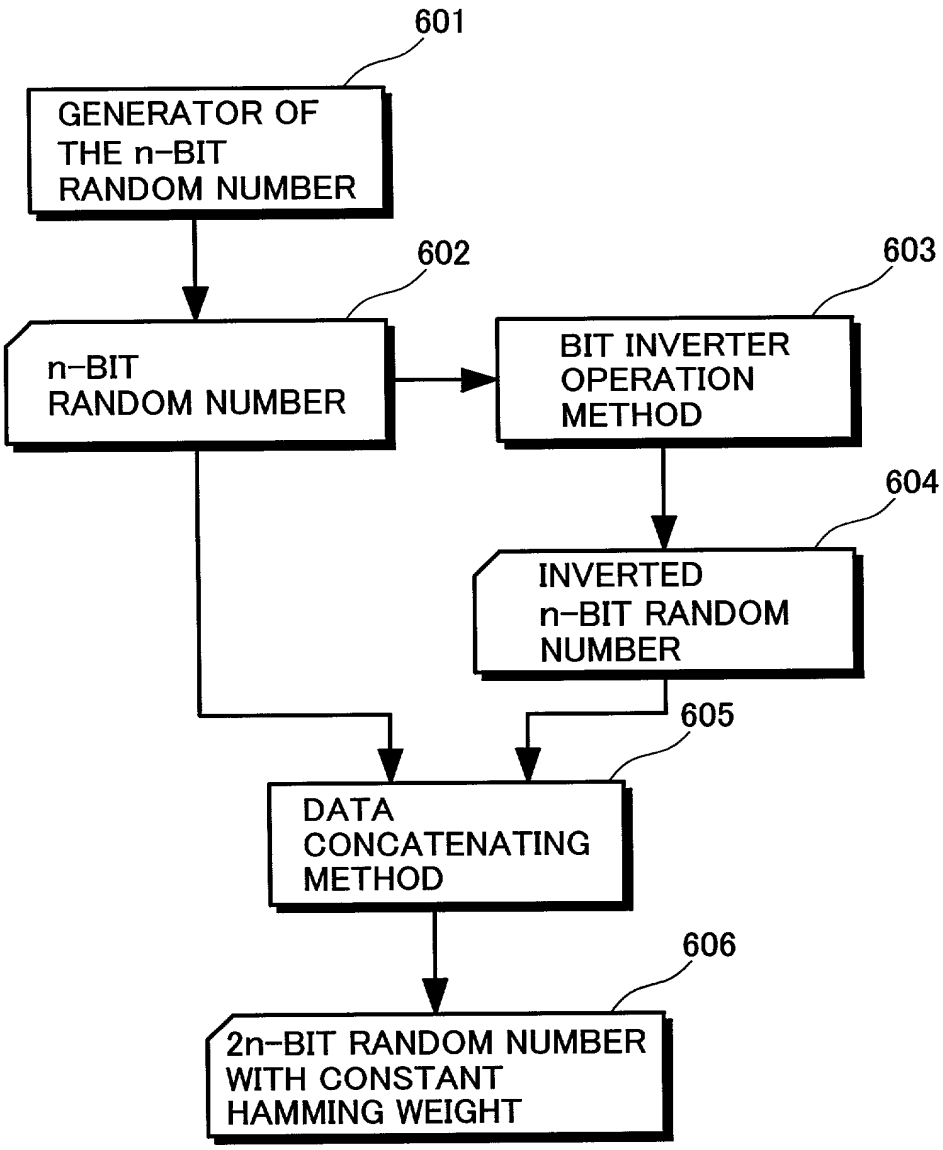

601
GENERATOR OF THE n-BIT RANDOM NUMBER
602
n-BIT RANDOM NUMBER
603
BIT INVERTER OPERATION METHOD
604
INVERTED n-BIT RANDOM NUMBER
605
DATA CONCATENATING METHOD
606
2n-BIT RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT

FIG. 7

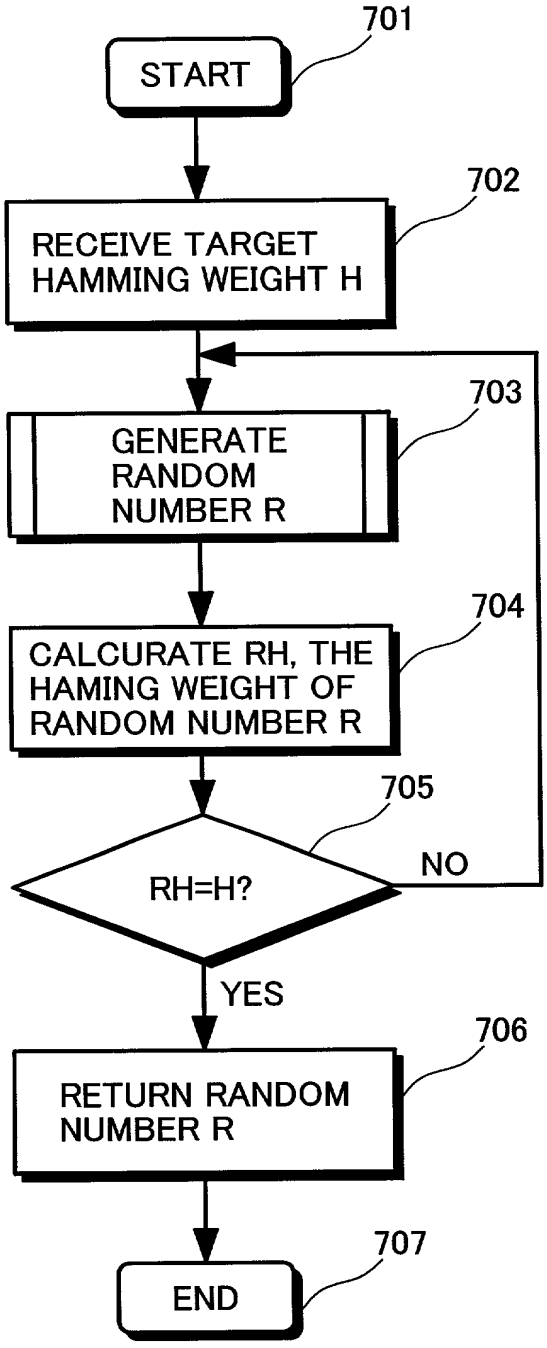

701
START
702
RECEIVE TARGET HAMMING WEIGHT H
703
GENERATE RANDOM NUMBER R
704
CALCURATE RH, THE HAMING WEIGHT OF RANDOM NUMBER R
705
RH=H?
NO
YES
706
RETURN RANDOM NUMBER R
707
END

FIG. 8

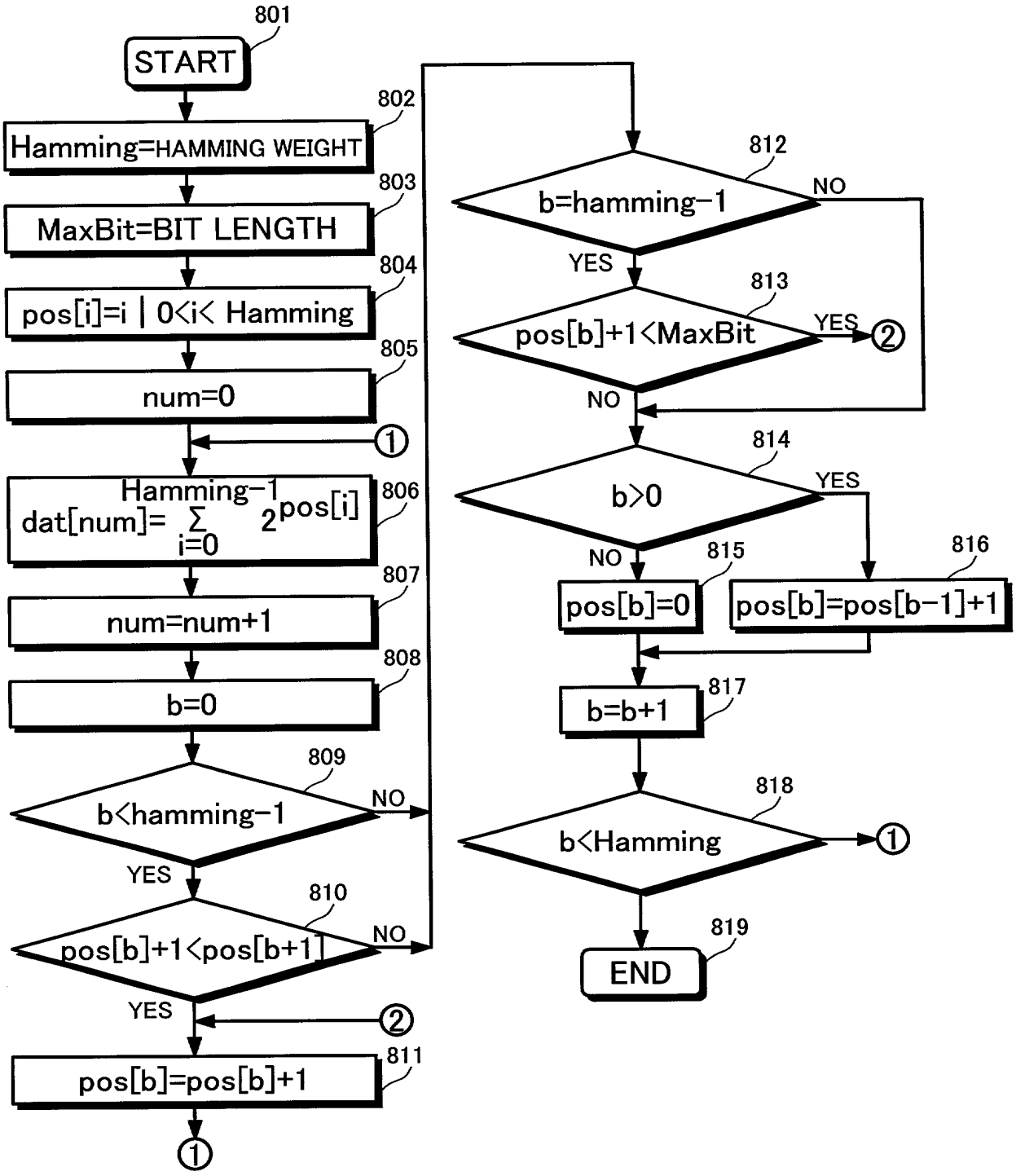

801
START
802
Hamming=HAMMING WEIGHT
803
MaxBit=BIT LENGTH
804
pos[i]=i | 0<i< Hamming
805
num=0
①
806
dat[num]= Σ 2^pos[i]
i=0
Hamming−1
807
num=num+1
808
b=0
809
b<hamming−1
NO
YES
810
pos[b]+1<pos[b+1]
NO
YES
②
811
pos[b]=pos[b]+1
①
812
b=hamming−1
NO
YES
813
pos[b]+1<MaxBit
YES
②
NO
814
b>0
YES
NO
815
pos[b]=0
816
pos[b]=pos[b−1]+1
817
b=b+1
818
b<Hamming
①
819
END

FIG. 9

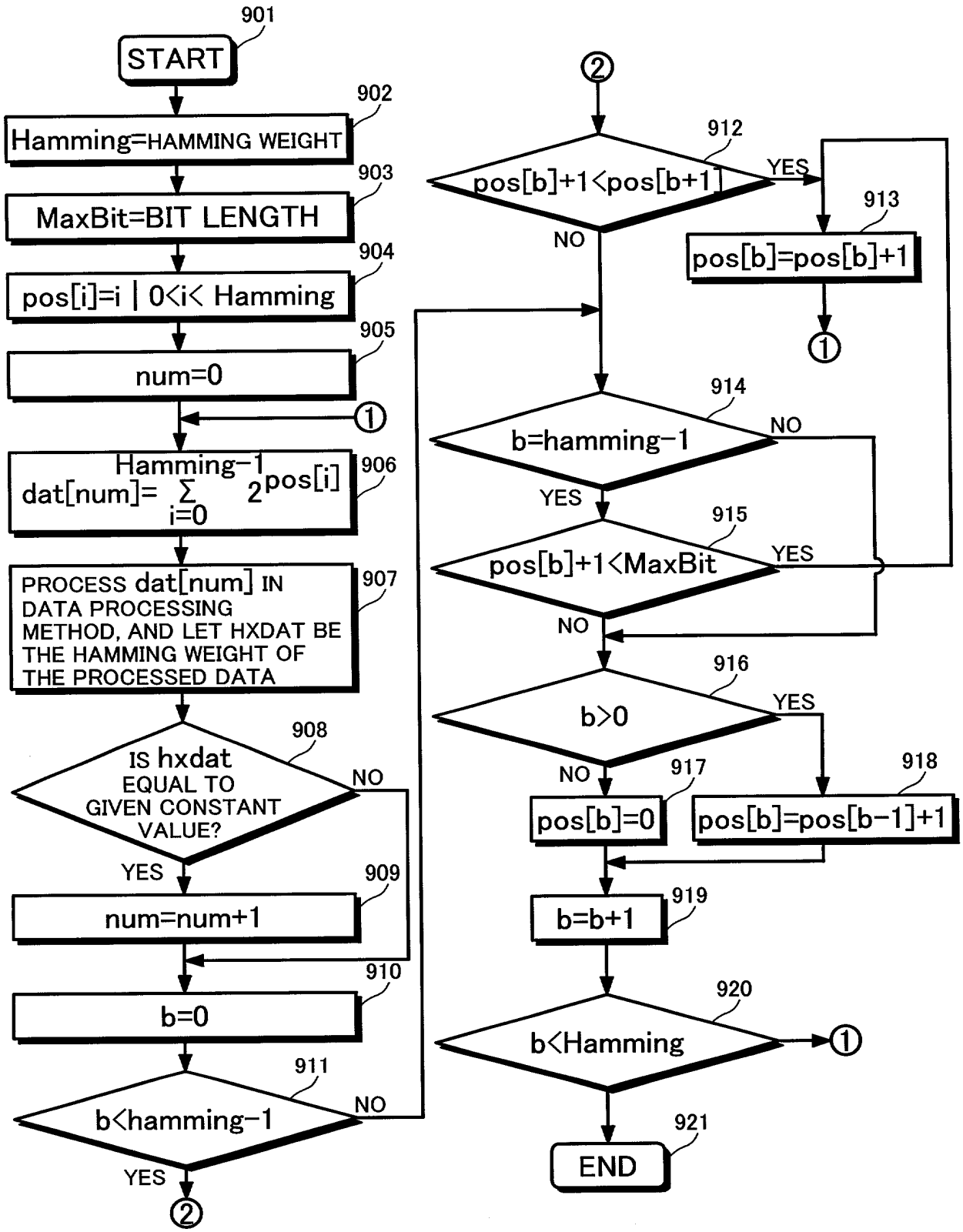

901
START
902
Hamming=HAMMING WEIGHT
903
MaxBit=BIT LENGTH
904
pos[i]=i | 0<i< Hamming
905
num=0
①
906
dat[num]= Σ 2^pos[i] (i=0 to Hamming−1)
907
PROCESS dat[num] IN DATA PROCESSING METHOD, AND LET HXDAT BE THE HAMMING WEIGHT OF THE PROCESSED DATA
908
IS hxdat EQUAL TO GIVEN CONSTANT VALUE?
NO
YES
909
num=num+1
910
b=0
911
b<hamming−1
NO
YES
②
②
912
pos[b]+1<pos[b+1]
YES
NO
913
pos[b]=pos[b]+1
①
914
b=hamming−1
NO
YES
915
pos[b]+1<MaxBit
YES
NO
916
b>0
YES
NO
917
pos[b]=0
918
pos[b]=pos[b−1]+1
919
b=b+1
920
b<Hamming
①
921
END

FIG. 10

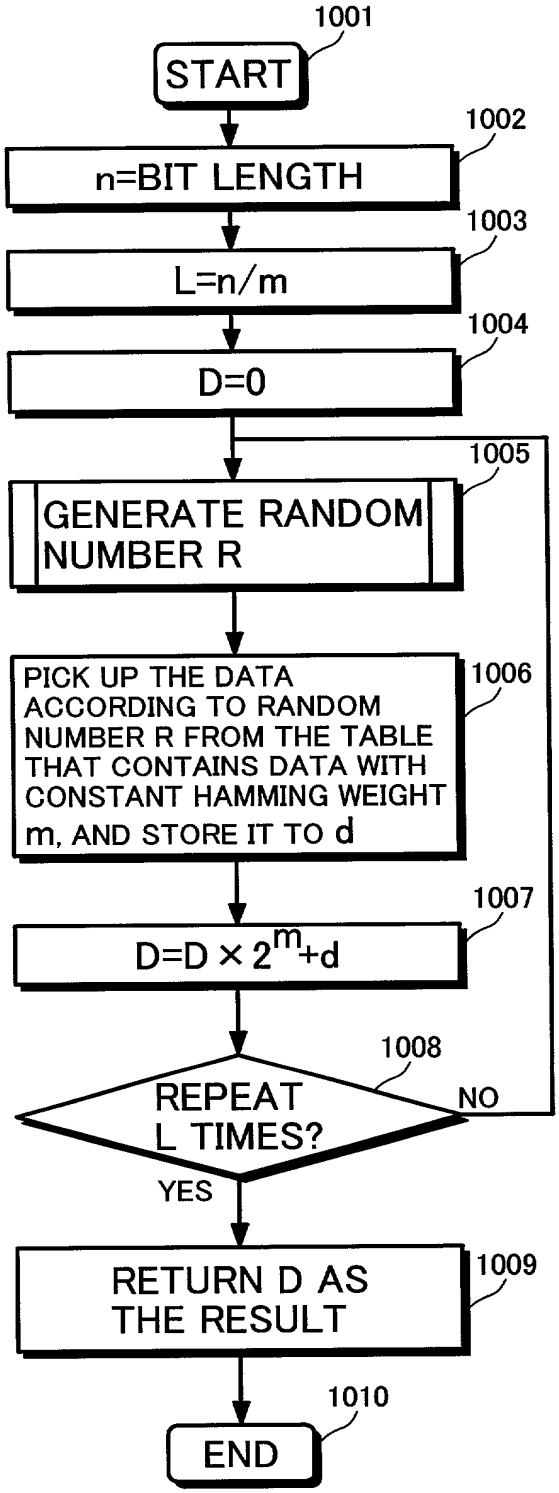

1001
START
1002
n=BIT LENGTH
1003
L=n/m
1004
D=0
1005
GENERATE RANDOM NUMBER R
1006
PICK UP THE DATA ACCORDING TO RANDOM NUMBER R FROM THE TABLE THAT CONTAINS DATA WITH CONSTANT HAMMING WEIGHT m, AND STORE IT TO d
1007
D=D × 2^m+d
1008
REPEAT L TIMES?
NO
YES
1009
RETURN D AS THE RESULT
1010
END

FIG. 11

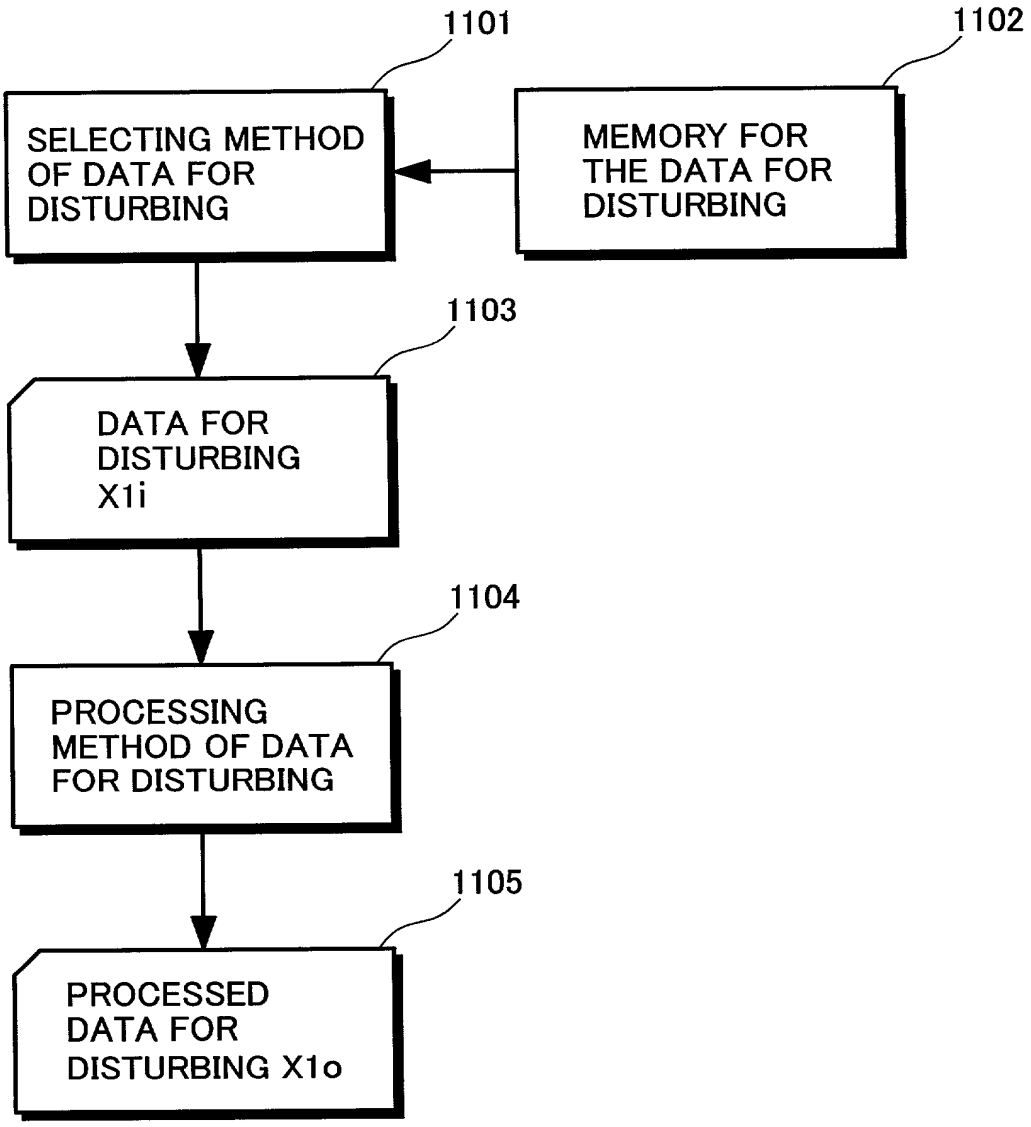

1101
1102
SELECTING METHOD OF DATA FOR DISTURBING
MEMORY FOR THE DATA FOR DISTURBING
1103
DATA FOR DISTURBING X1i
1104
PROCESSING METHOD OF DATA FOR DISTURBING
1105
PROCESSED DATA FOR DISTURBING X1o

FIG. 12

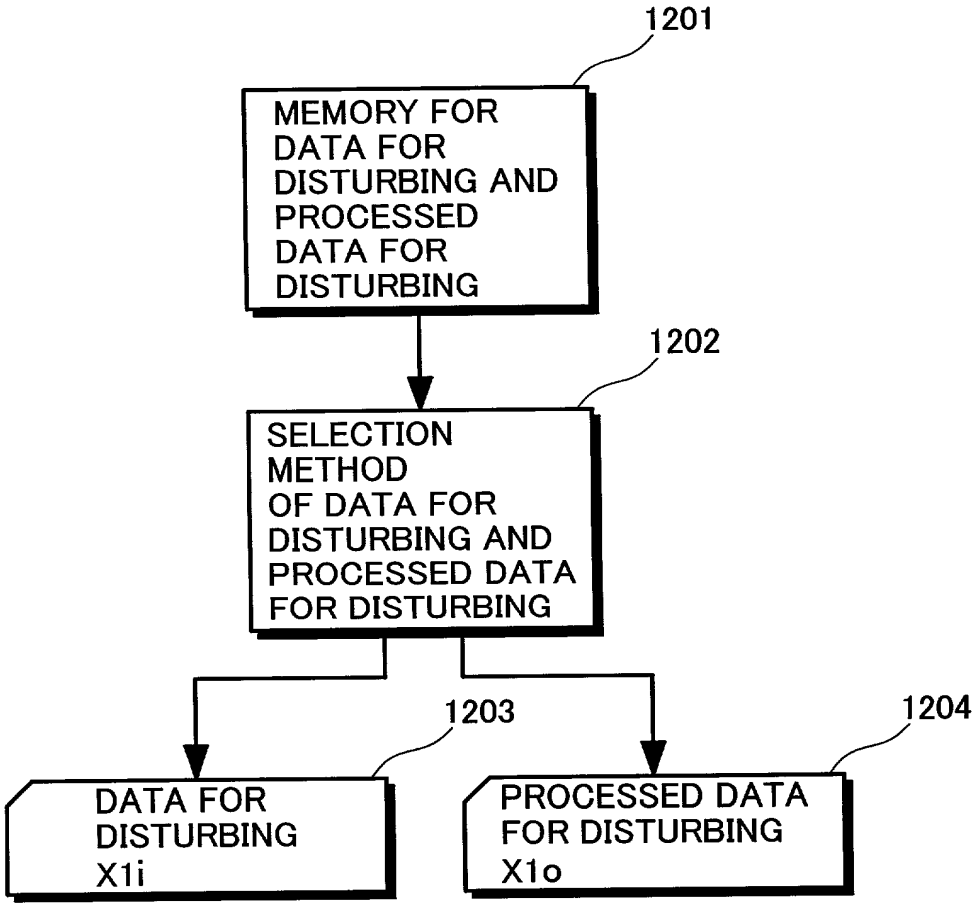

1201
MEMORY FOR DATA FOR DISTURBING AND PROCESSED DATA FOR DISTURBING
1202
SELECTION METHOD OF DATA FOR DISTURBING AND PROCESSED DATA FOR DISTURBING
1203
DATA FOR DISTURBING X1i
1204
PROCESSED DATA FOR DISTURBING X1o

FIG. 13

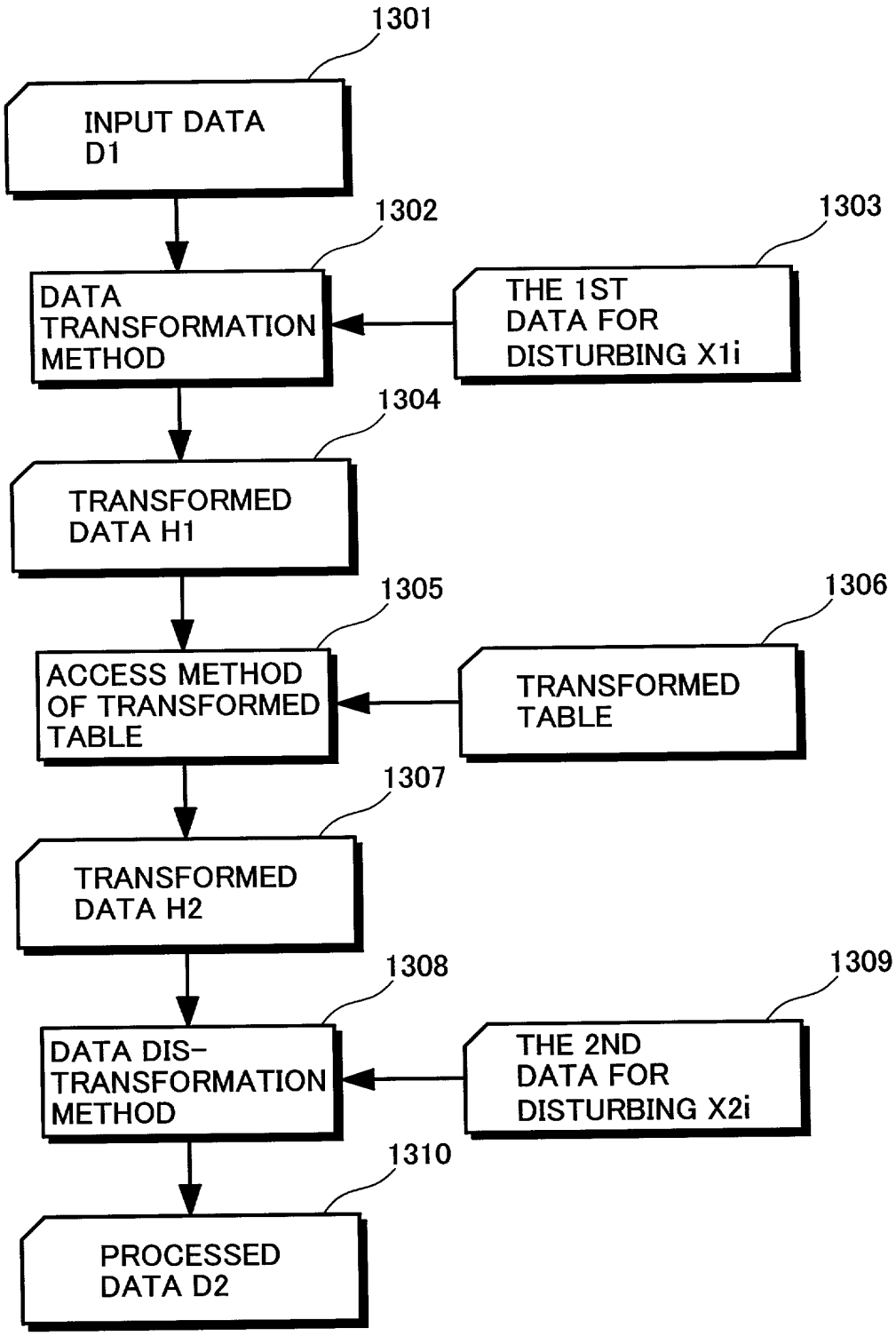

1301
INPUT DATA D1
1302
DATA TRANSFORMATION METHOD
1303
THE 1ST DATA FOR DISTURBING X1i
1304
TRANSFORMED DATA H1
1305
ACCESS METHOD OF TRANSFORMED TABLE
1306
TRANSFORMED TABLE
1307
TRANSFORMED DATA H2
1308
DATA DIS-TRANSFORMATION METHOD
1309
THE 2ND DATA FOR DISTURBING X2i
1310
PROCESSED DATA D2

FIG. 14

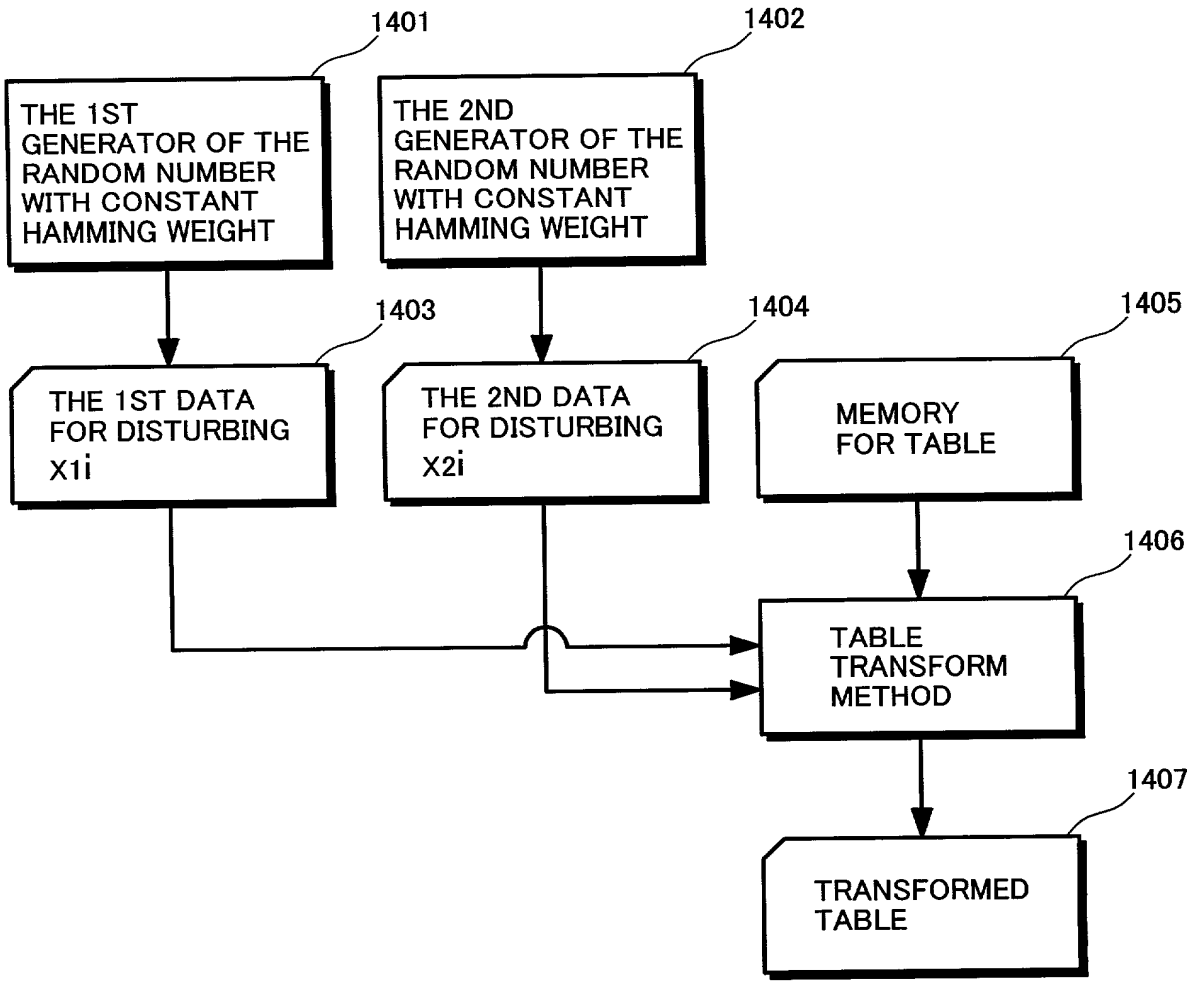

1401
THE 1ST GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
1402
THE 2ND GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
1403
THE 1ST DATA FOR DISTURBING X1i
1404
THE 2ND DATA FOR DISTURBING X2i
1405
MEMORY FOR TABLE
1406
TABLE TRANSFORM METHOD
1407
TRANSFORMED TABLE

FIG. 15

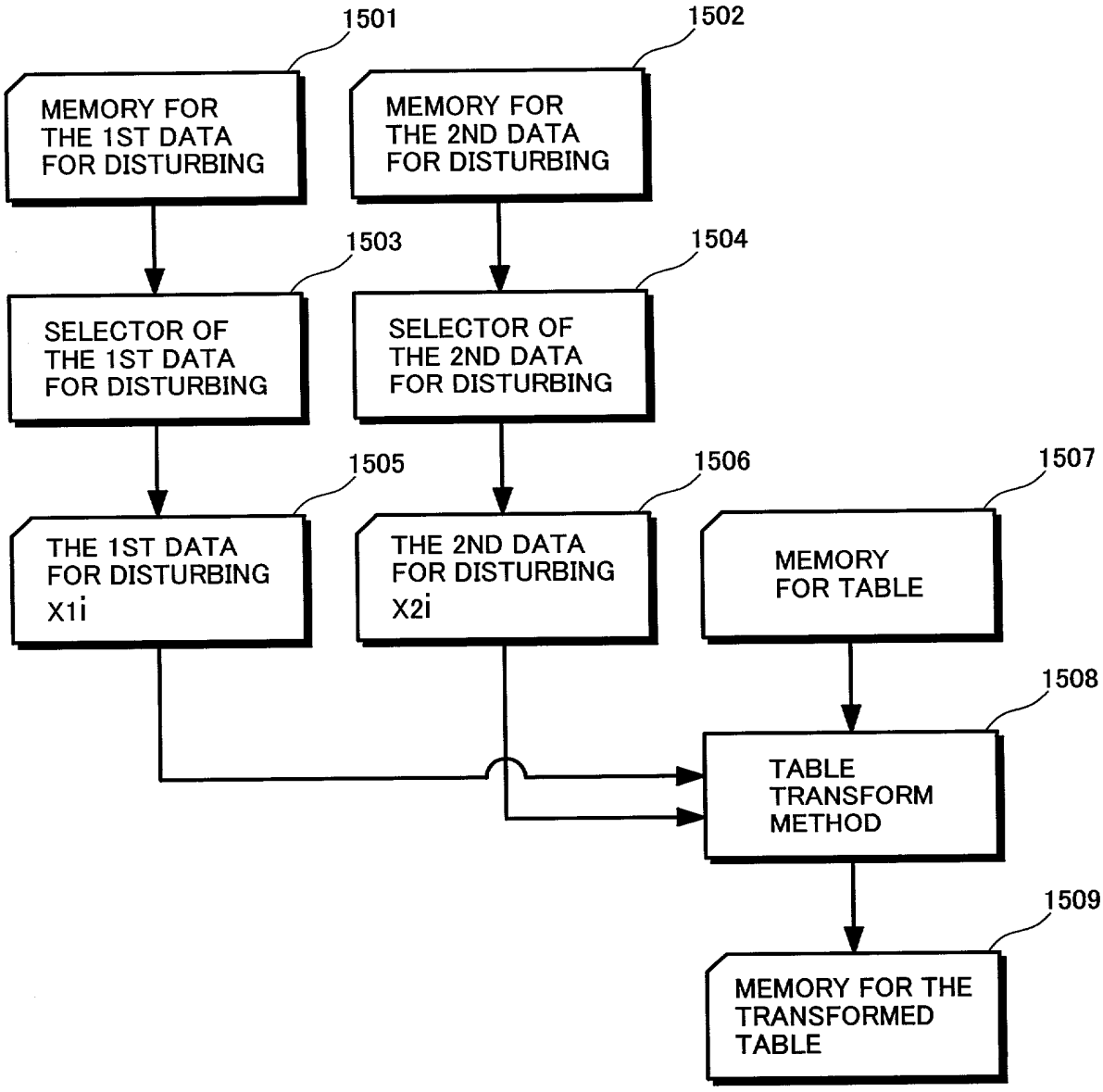

1501
MEMORY FOR THE 1ST DATA FOR DISTURBING
1502
MEMORY FOR THE 2ND DATA FOR DISTURBING
1503
SELECTOR OF THE 1ST DATA FOR DISTURBING
1504
SELECTOR OF THE 2ND DATA FOR DISTURBING
1505
THE 1ST DATA FOR DISTURBING X1i
1506
THE 2ND DATA FOR DISTURBING X2i
1507
MEMORY FOR TABLE
1508
TABLE TRANSFORM METHOD
1509
MEMORY FOR THE TRANSFORMED TABLE

FIG. 16

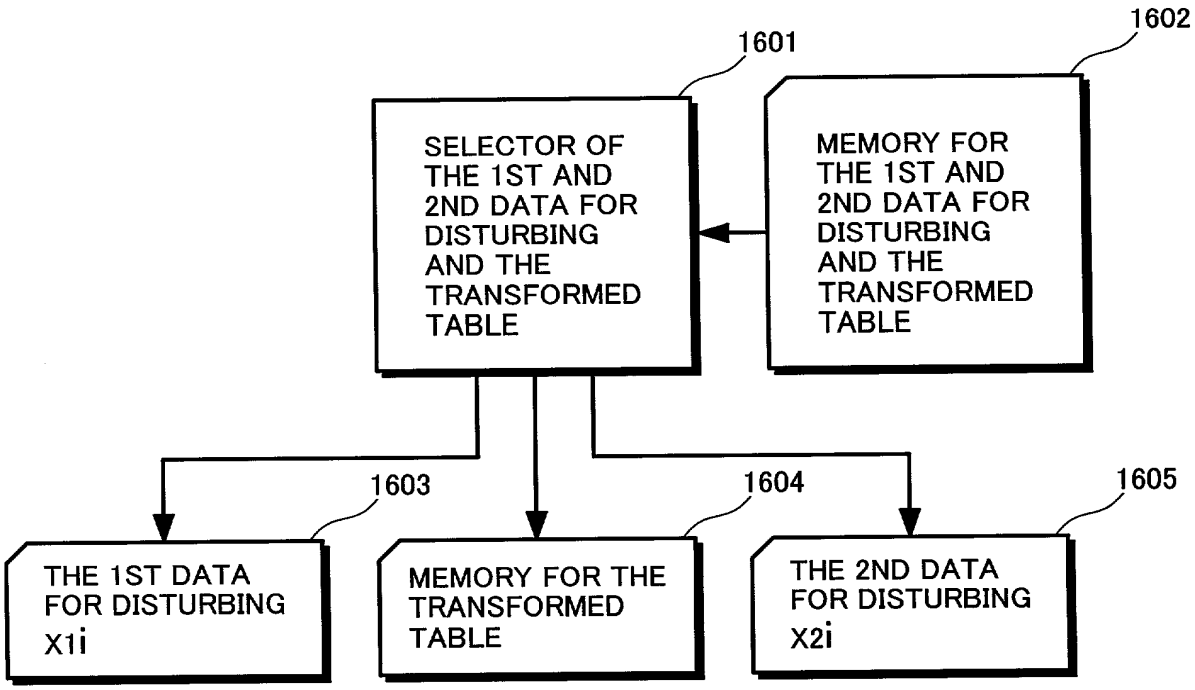

1601
1602
SELECTOR OF THE 1ST AND 2ND DATA FOR DISTURBING AND THE TRANSFORMED TABLE
MEMORY FOR THE 1ST AND 2ND DATA FOR DISTURBING AND THE TRANSFORMED TABLE
1603
1604
1605
THE 1ST DATA FOR DISTURBING X1i
MEMORY FOR THE TRANSFORMED TABLE
THE 2ND DATA FOR DISTURBING X2i

FIG. 17

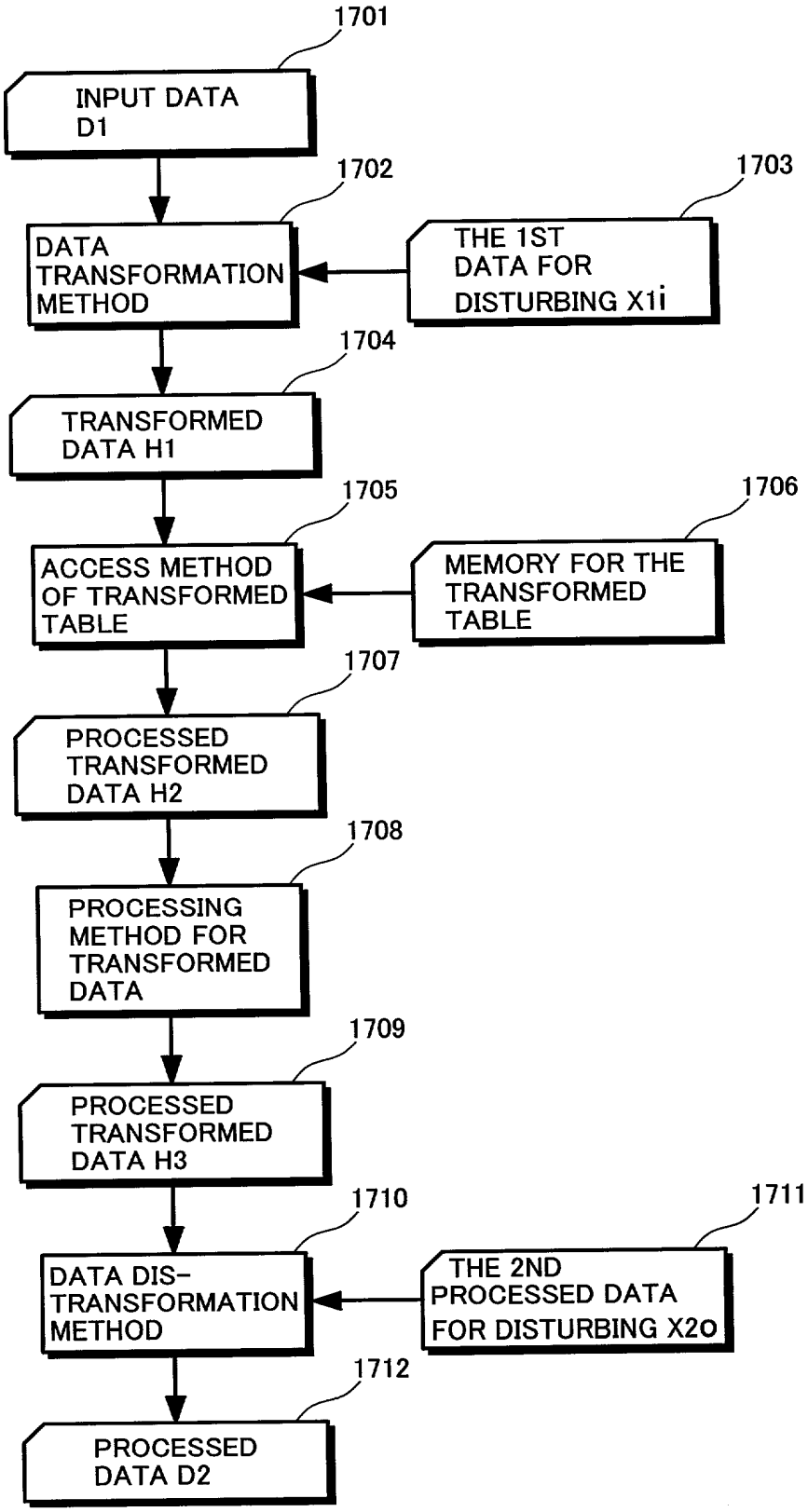

1701
INPUT DATA D1
1702
DATA TRANSFORMATION METHOD
1703
THE 1ST DATA FOR DISTURBING X1i
1704
TRANSFORMED DATA H1
1705
ACCESS METHOD OF TRANSFORMED TABLE
1706
MEMORY FOR THE TRANSFORMED TABLE
1707
PROCESSED TRANSFORMED DATA H2
1708
PROCESSING METHOD FOR TRANSFORMED DATA
1709
PROCESSED TRANSFORMED DATA H3
1710
DATA DIS-TRANSFORMATION METHOD
1711
THE 2ND PROCESSED DATA FOR DISTURBING X2o
1712
PROCESSED DATA D2

FIG. 18

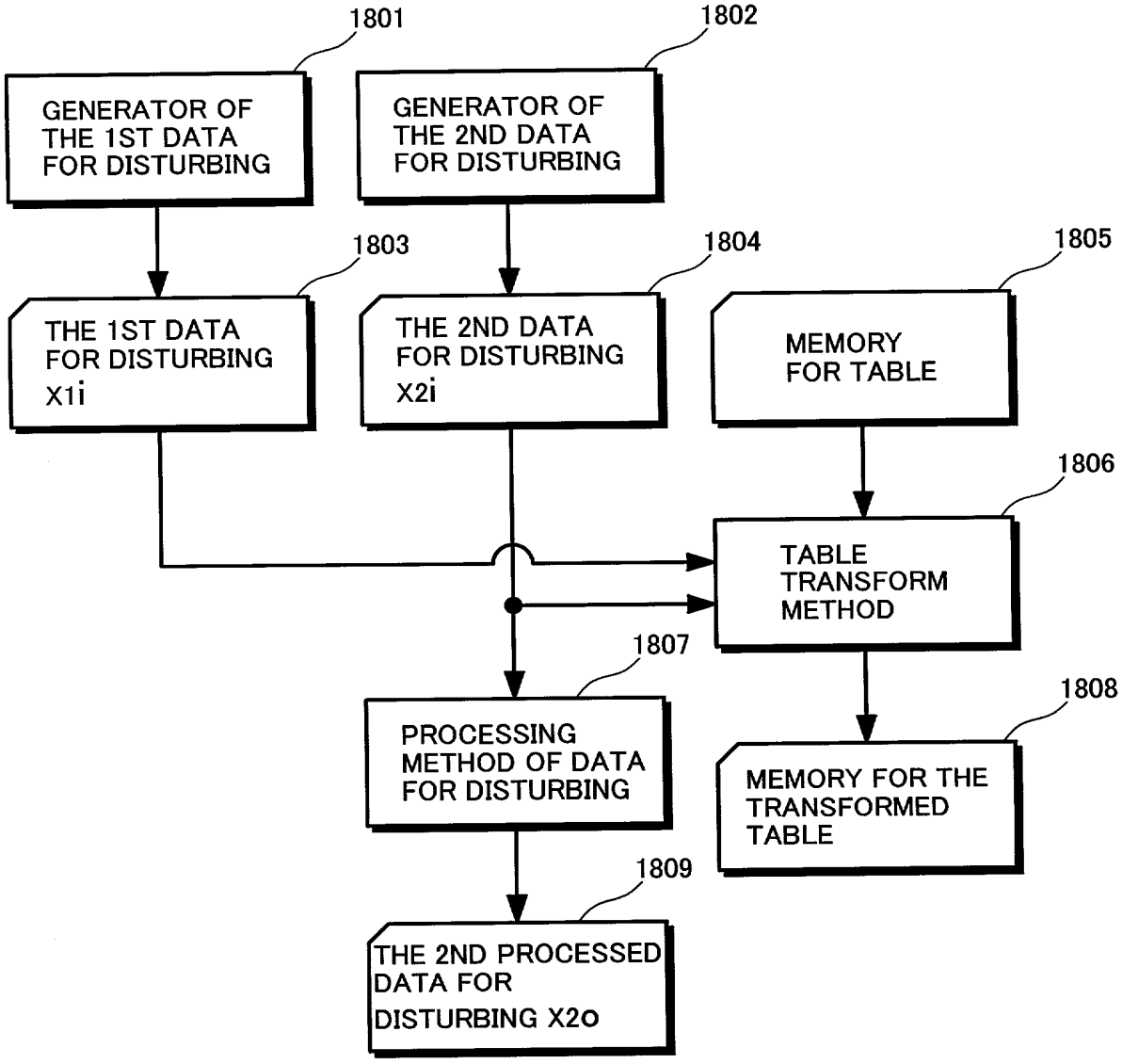

1801
GENERATOR OF THE 1ST DATA FOR DISTURBING
1802
GENERATOR OF THE 2ND DATA FOR DISTURBING
1803
THE 1ST DATA FOR DISTURBING X1i
1804
THE 2ND DATA FOR DISTURBING X2i
1805
MEMORY FOR TABLE
1806
TABLE TRANSFORM METHOD
1807
PROCESSING METHOD OF DATA FOR DISTURBING
1808
MEMORY FOR THE TRANSFORMED TABLE
1809
THE 2ND PROCESSED DATA FOR DISTURBING X2o

FIG. 19

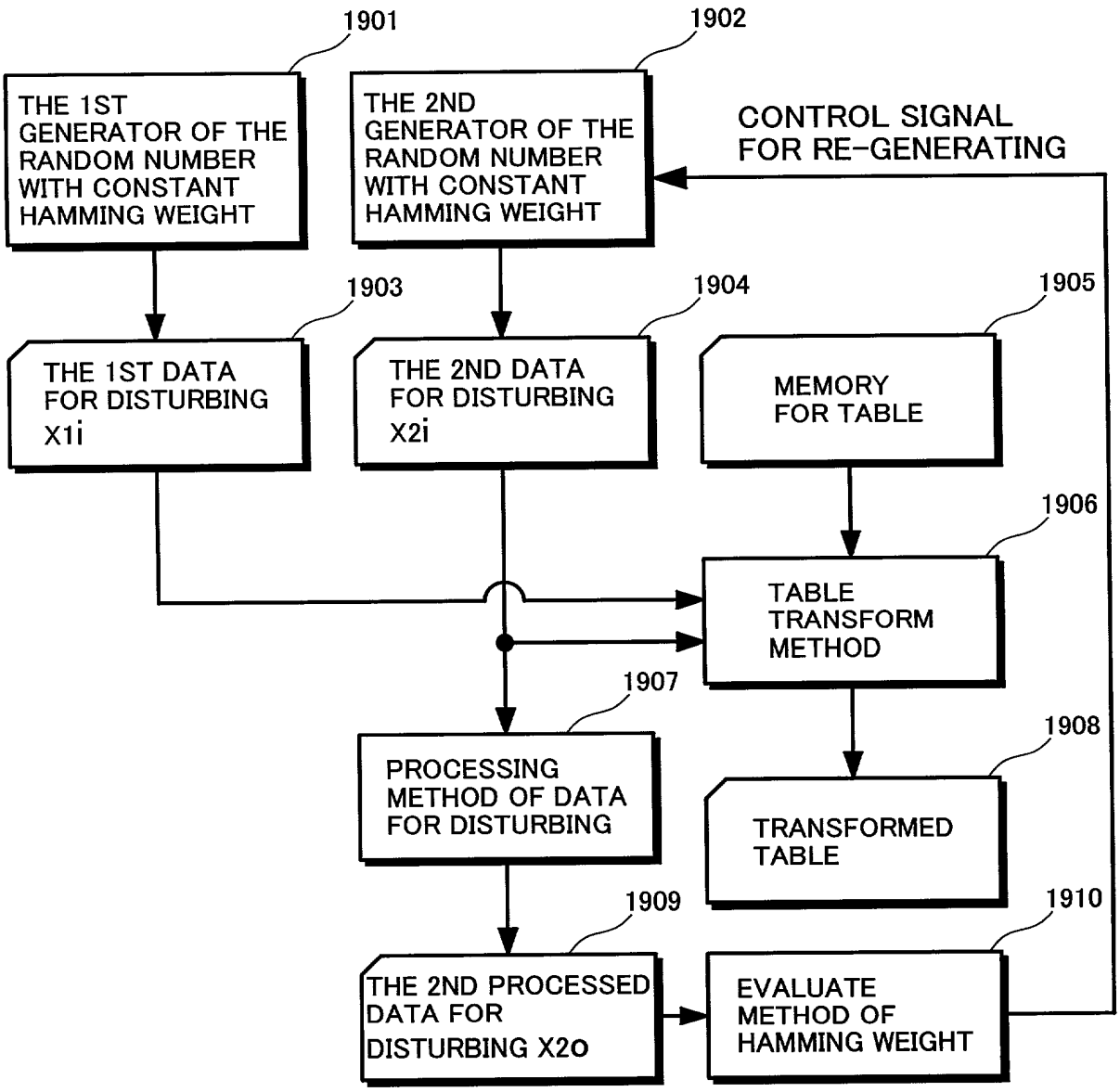

1901
1902
THE 1ST GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
THE 2ND GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
CONTROL SIGNAL FOR RE-GENERATING
1903
1904
1905
THE 1ST DATA FOR DISTURBING X1i
THE 2ND DATA FOR DISTURBING X2i
MEMORY FOR TABLE
1906
TABLE TRANSFORM METHOD
1907
1908
PROCESSING METHOD OF DATA FOR DISTURBING
TRANSFORMED TABLE
1909
1910
THE 2ND PROCESSED DATA FOR DISTURBING X2o
EVALUATE METHOD OF HAMMING WEIGHT

FIG. 20

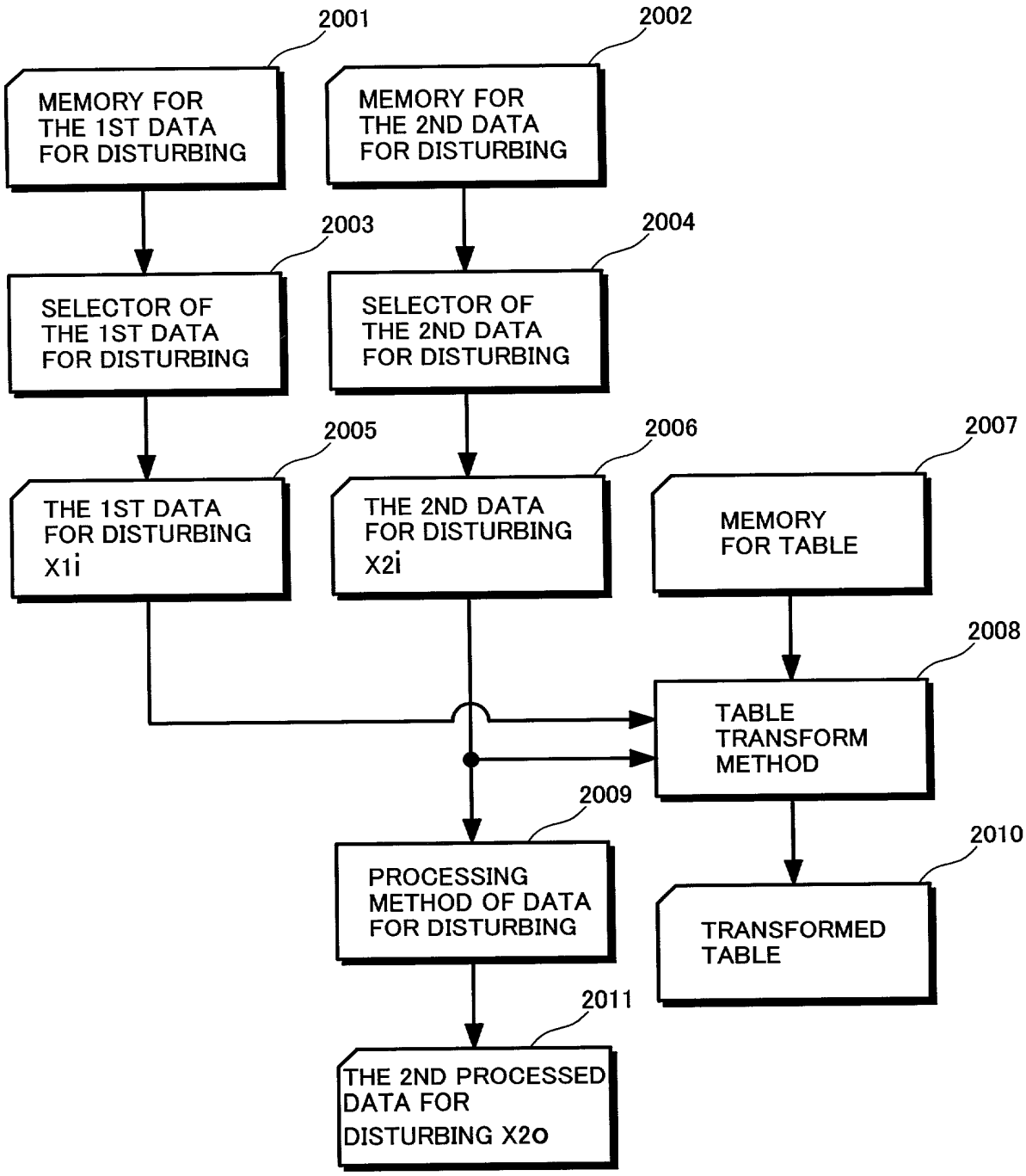

2001
MEMORY FOR THE 1ST DATA FOR DISTURBING
2002
MEMORY FOR THE 2ND DATA FOR DISTURBING
2003
SELECTOR OF THE 1ST DATA FOR DISTURBING
2004
SELECTOR OF THE 2ND DATA FOR DISTURBING
2005
THE 1ST DATA FOR DISTURBING X1i
2006
THE 2ND DATA FOR DISTURBING X2i
2007
MEMORY FOR TABLE
2008
TABLE TRANSFORM METHOD
2009
PROCESSING METHOD OF DATA FOR DISTURBING
2010
TRANSFORMED TABLE
2011
THE 2ND PROCESSED DATA FOR DISTURBING X2o

FIG. 21

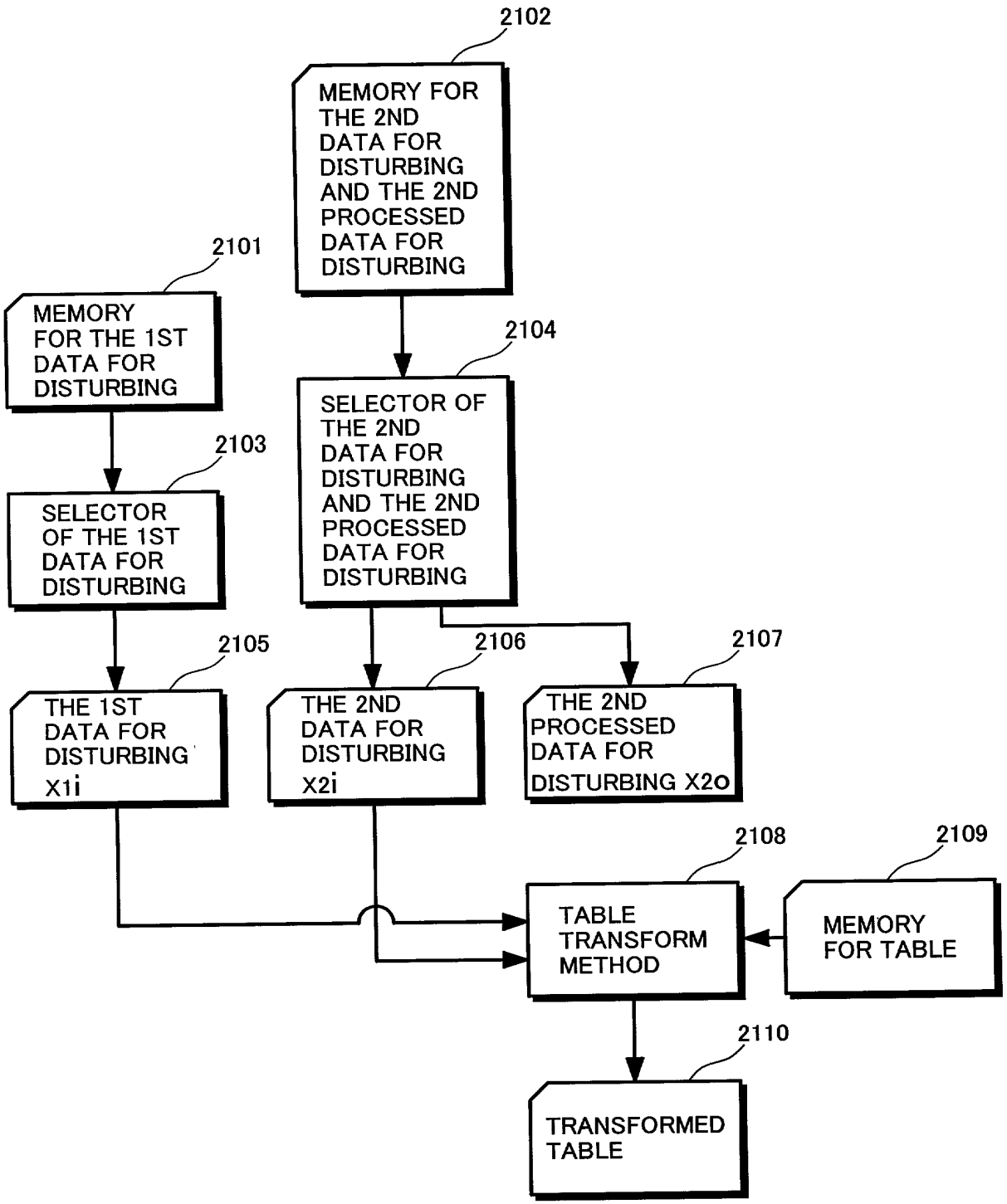

2102
MEMORY FOR THE 2ND DATA FOR DISTURBING AND THE 2ND PROCESSED DATA FOR DISTURBING
2101
MEMORY FOR THE 1ST DATA FOR DISTURBING
2104
SELECTOR OF THE 2ND DATA FOR DISTURBING AND THE 2ND PROCESSED DATA FOR DISTURBING
2103
SELECTOR OF THE 1ST DATA FOR DISTURBING
2105
2106
2107
THE 1ST DATA FOR DISTURBING X1i
THE 2ND DATA FOR DISTURBING X2i
THE 2ND PROCESSED DATA FOR DISTURBING X2o
2108
2109
TABLE TRANSFORM METHOD
MEMORY FOR TABLE
2110
TRANSFORMED TABLE

FIG. 22

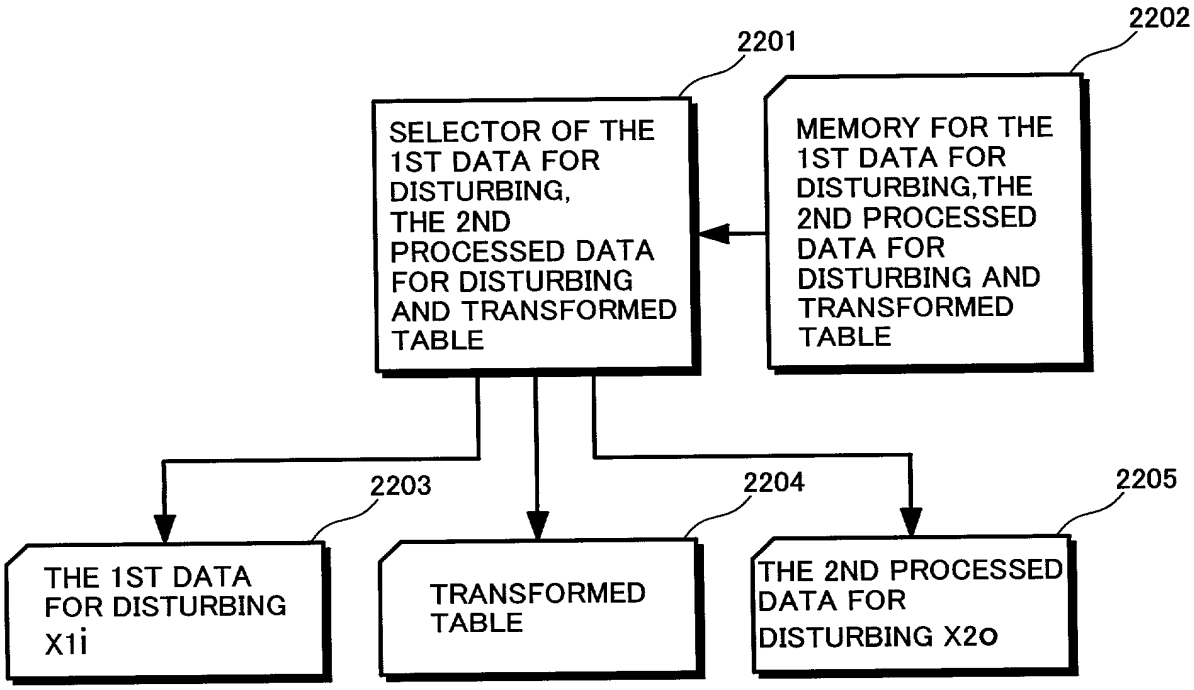

2201
2202
SELECTOR OF THE 1ST DATA FOR DISTURBING, THE 2ND PROCESSED DATA FOR DISTURBING AND TRANSFORMED TABLE
MEMORY FOR THE 1ST DATA FOR DISTURBING,THE 2ND PROCESSED DATA FOR DISTURBING AND TRANSFORMED TABLE
2203
2204
2205
THE 1ST DATA FOR DISTURBING X1i
TRANSFORMED TABLE
THE 2ND PROCESSED DATA FOR DISTURBING X2o

FIG. 23

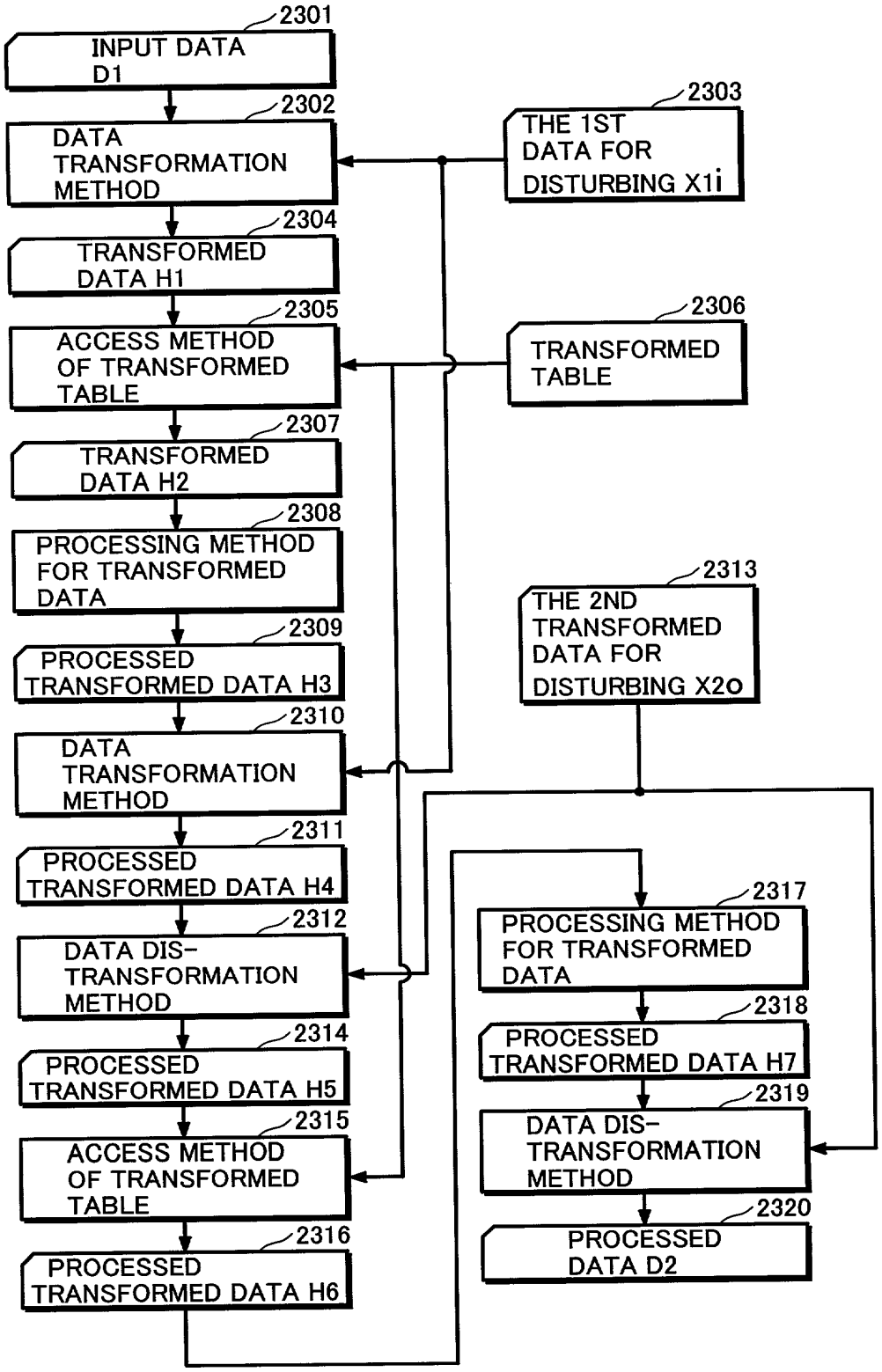
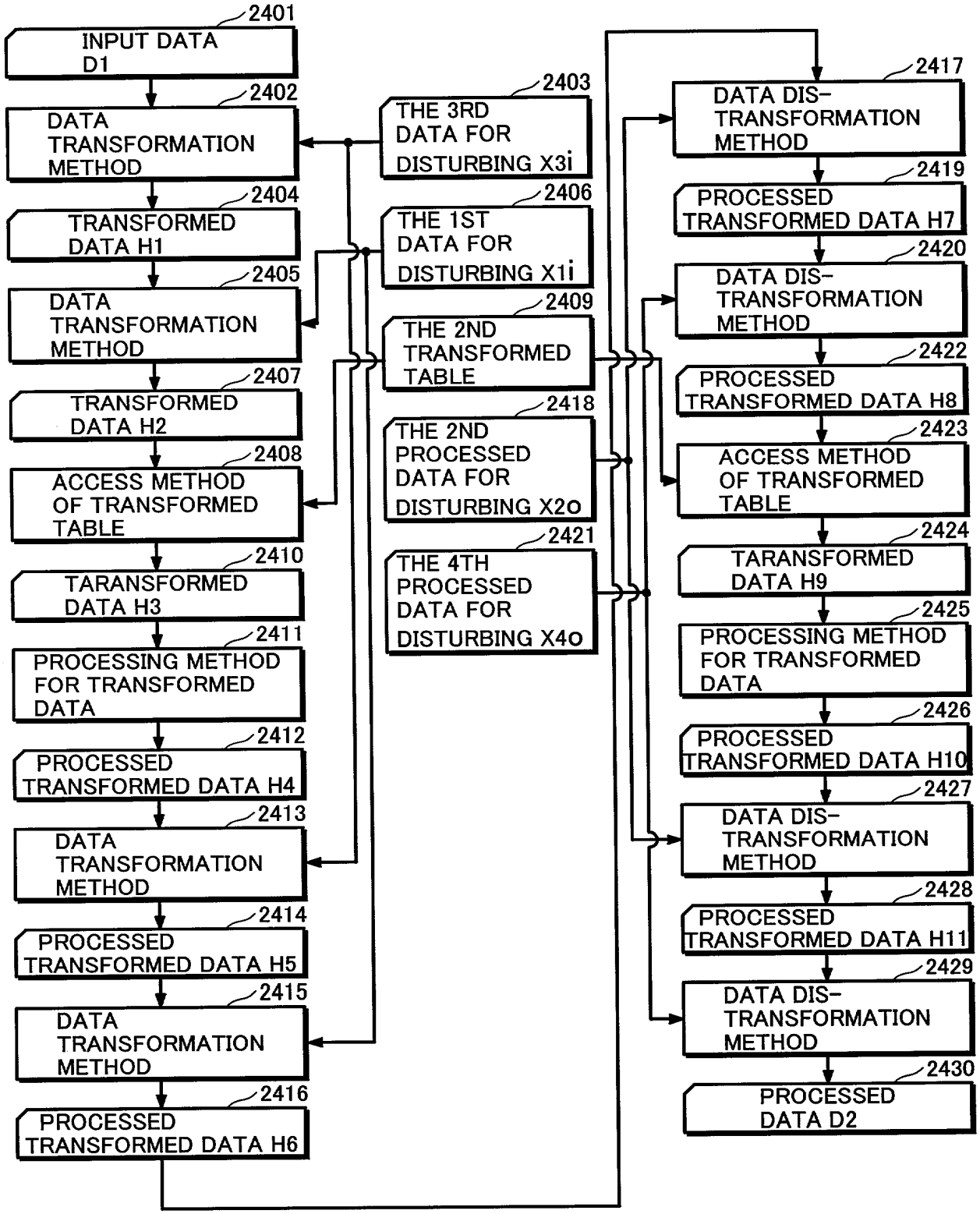

2301
INPUT DATA D1
2302
DATA TRANSFORMATION METHOD
2303
THE 1ST DATA FOR DISTURBING X1i
2304
TRANSFORMED DATA H1
2305
ACCESS METHOD OF TRANSFORMED TABLE
2306
TRANSFORMED TABLE
2307
TRANSFORMED DATA H2
2308
PROCESSING METHOD FOR TRANSFORMED DATA
2309
PROCESSED TRANSFORMED DATA H3
2310
DATA TRANSFORMATION METHOD
2311
PROCESSED TRANSFORMED DATA H4
2312
DATA DIS-TRANSFORMATION METHOD
2313
THE 2ND TRANSFORMED DATA FOR DISTURBING X2o
2314
PROCESSED TRANSFORMED DATA H5
2315
ACCESS METHOD OF TRANSFORMED TABLE
2316
PROCESSED TRANSFORMED DATA H6
2317
PROCESSING METHOD FOR TRANSFORMED DATA
2318
PROCESSED TRANSFORMED DATA H7
2319
DATA DIS-TRANSFORMATION METHOD
2320
PROCESSED DATA D2

FIG. 24



US 6,684,082 B1

FIG. 25

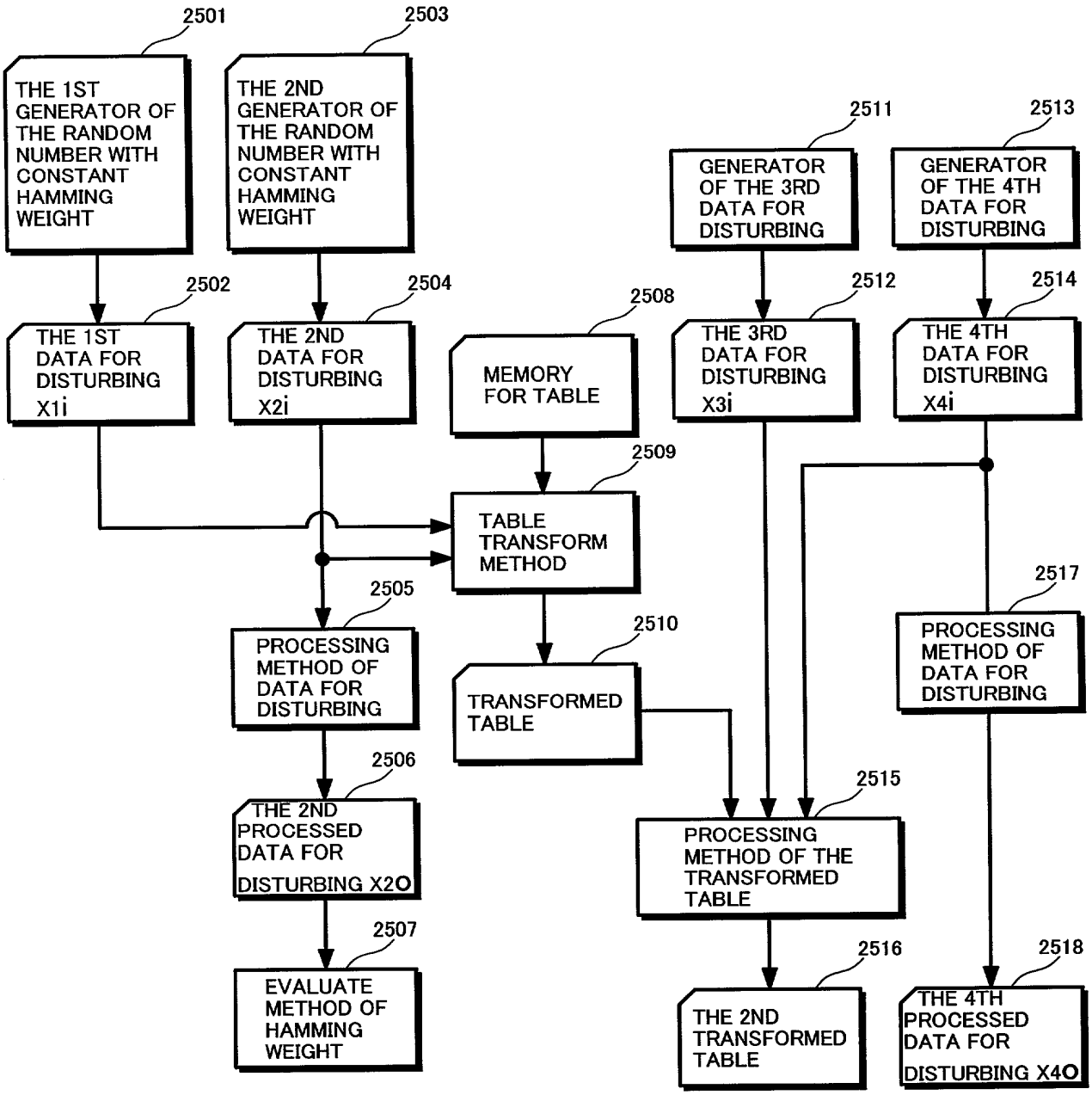

2501
THE 1ST GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
2503
THE 2ND GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
2511
GENERATOR OF THE 3RD DATA FOR DISTURBING
2513
GENERATOR OF THE 4TH DATA FOR DISTURBING
2502
THE 1ST DATA FOR DISTURBING X1i
2504
THE 2ND DATA FOR DISTURBING X2i
2508
MEMORY FOR TABLE
2512
THE 3RD DATA FOR DISTURBING X3i
2514
THE 4TH DATA FOR DISTURBING X4i
2509
TABLE TRANSFORM METHOD
2505
PROCESSING METHOD OF DATA FOR DISTURBING
2510
TRANSFORMED TABLE
2517
PROCESSING METHOD OF DATA FOR DISTURBING
2506
THE 2ND PROCESSED DATA FOR DISTURBING X2O
2515
PROCESSING METHOD OF THE TRANSFORMED TABLE
2507
EVALUATE METHOD OF HAMMING WEIGHT
2516
THE 2ND TRANSFORMED TABLE
2518
THE 4TH PROCESSED DATA FOR DISTURBING X4O

FIG. 26

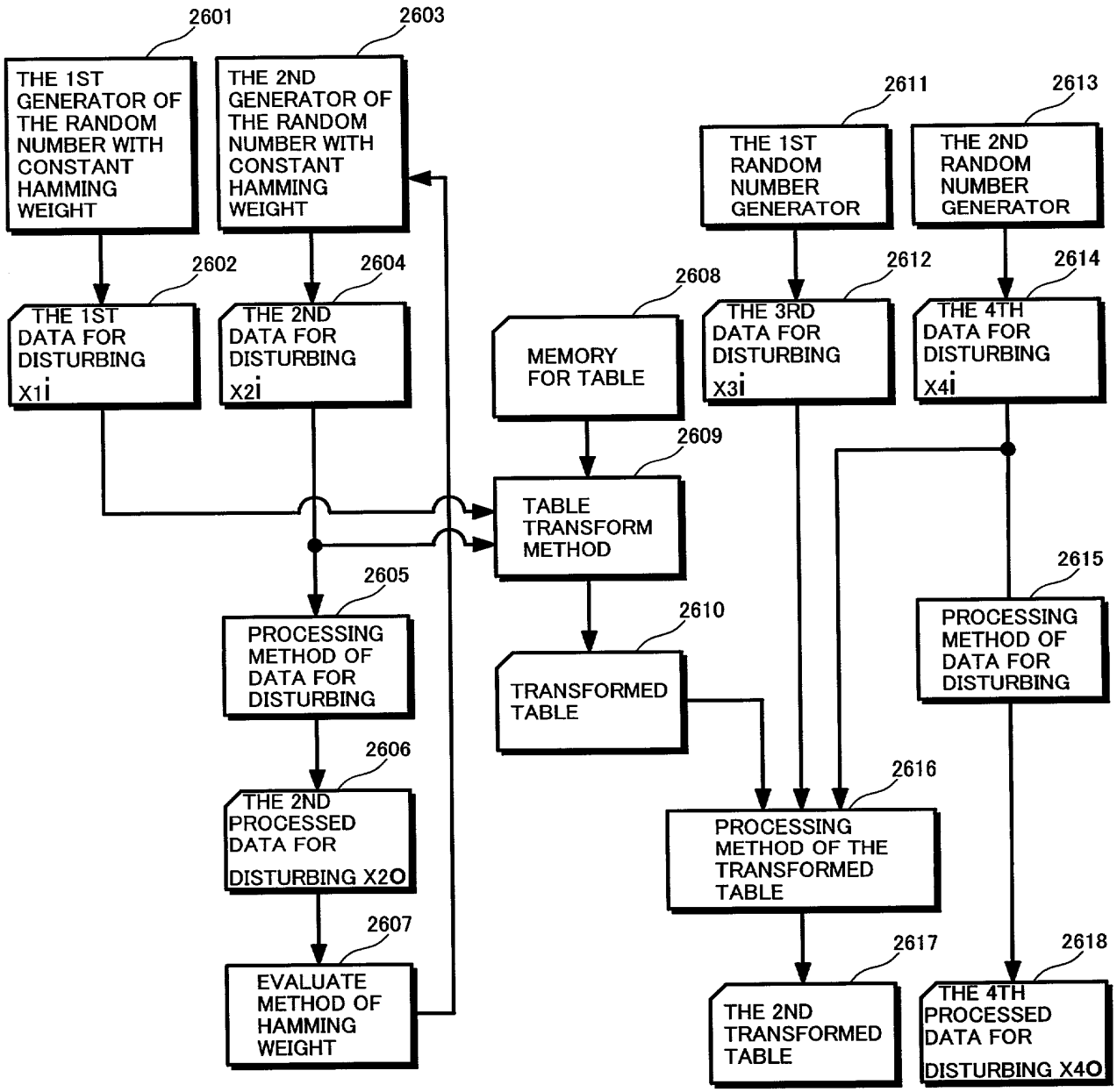
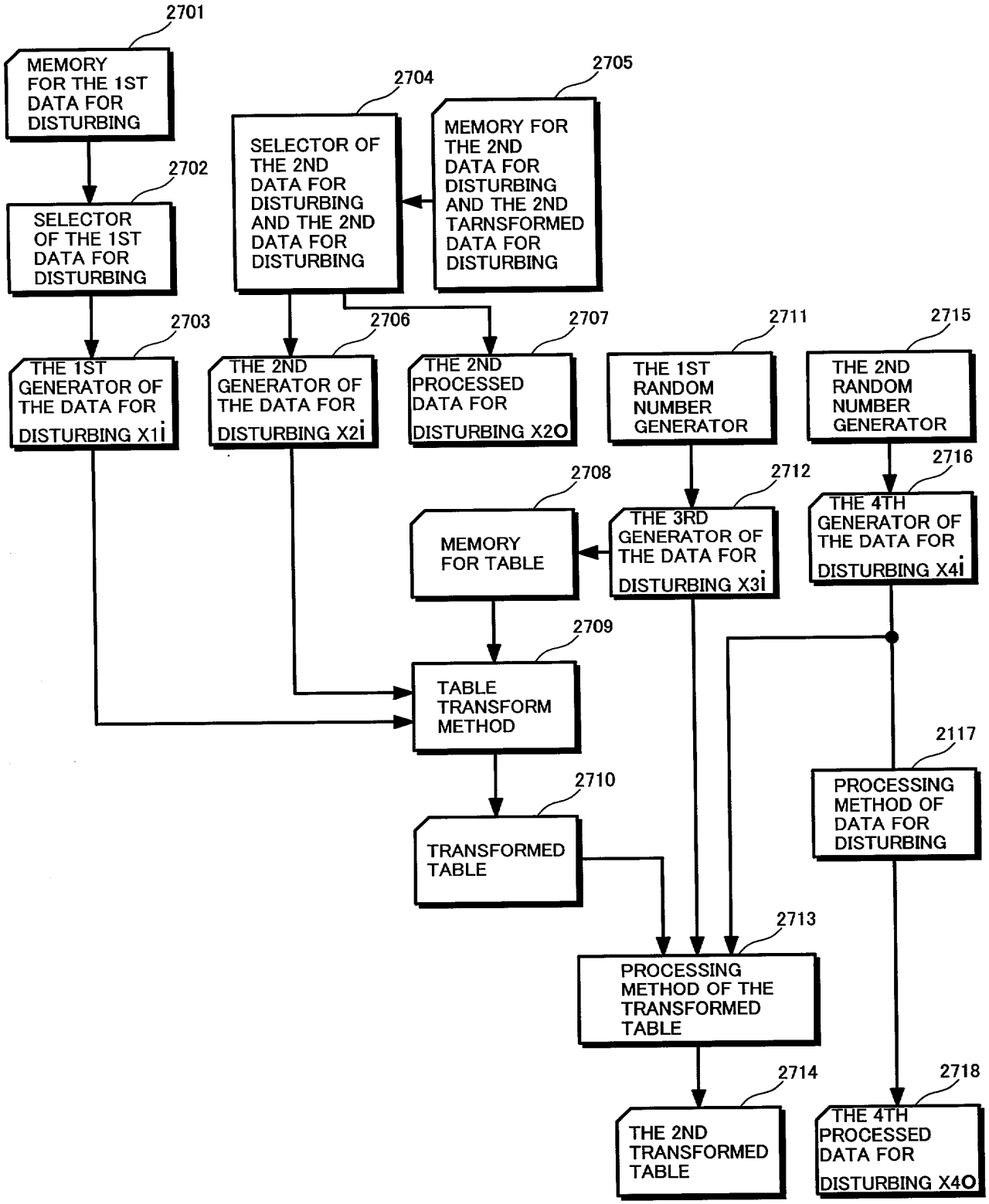

2601
THE 1ST GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
2603
THE 2ND GENERATOR OF THE RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
2611
THE 1ST RANDOM NUMBER GENERATOR
2613
THE 2ND RANDOM NUMBER GENERATOR
2602
THE 1ST DATA FOR DISTURBING X1i
2604
THE 2ND DATA FOR DISTURBING X2i
2608
MEMORY FOR TABLE
2612
THE 3RD DATA FOR DISTURBING X3i
2614
THE 4TH DATA FOR DISTURBING X4i
2609
TABLE TRANSFORM METHOD
2605
PROCESSING METHOD OF DATA FOR DISTURBING
2610
TRANSFORMED TABLE
2615
PROCESSING METHOD OF DATA FOR DISTURBING
2606
THE 2ND PROCESSED DATA FOR DISTURBING X2O
2616
PROCESSING METHOD OF THE TRANSFORMED TABLE
2607
EVALUATE METHOD OF HAMMING WEIGHT
2617
THE 2ND TRANSFORMED TABLE
2618
THE 4TH PROCESSED DATA FOR DISTURBING X4O

FIG. 27



US 6,950,523 B2

FIG. 28

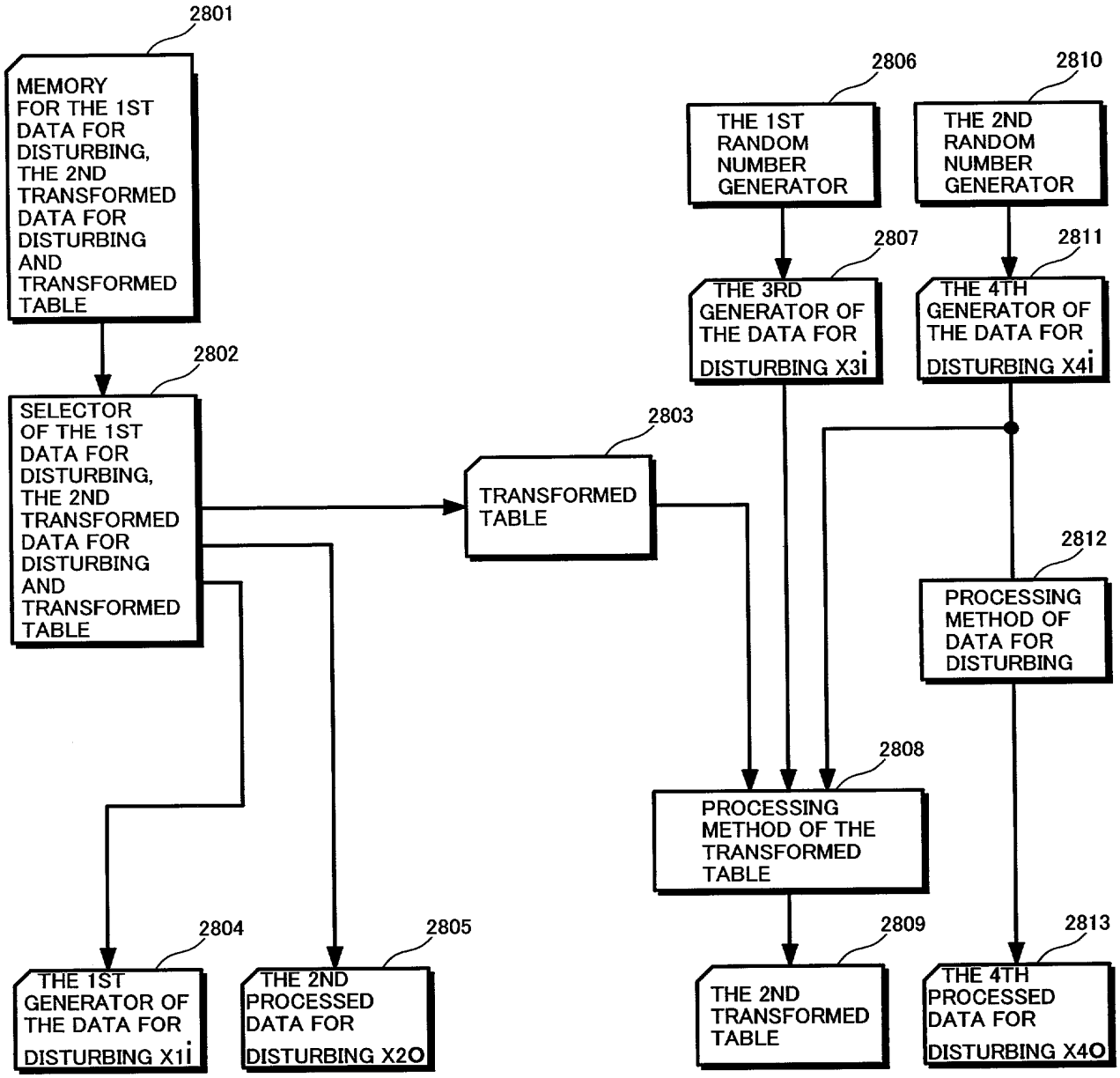

2801
MEMORY FOR THE 1ST DATA FOR DISTURBING, THE 2ND TRANSFORMED DATA FOR DISTURBING AND TRANSFORMED TABLE
2802
SELECTOR OF THE 1ST DATA FOR DISTURBING, THE 2ND TRANSFORMED DATA FOR DISTURBING AND TRANSFORMED TABLE
2803
TRANSFORMED TABLE
2804
THE 1ST GENERATOR OF THE DATA FOR DISTURBING X1i
2805
THE 2ND PROCESSED DATA FOR DISTURBING X2O
2806
THE 1ST RANDOM NUMBER GENERATOR
2807
THE 3RD GENERATOR OF THE DATA FOR DISTURBING X3i
2808
PROCESSING METHOD OF THE TRANSFORMED TABLE
2809
THE 2ND TRANSFORMED TABLE
2810
THE 2ND RANDOM NUMBER GENERATOR
2811
THE 4TH GENERATOR OF THE DATA FOR DISTURBING X4i
2812
PROCESSING METHOD OF DATA FOR DISTURBING
2813
THE 4TH PROCESSED DATA FOR DISTURBING X4O

FIG. 29

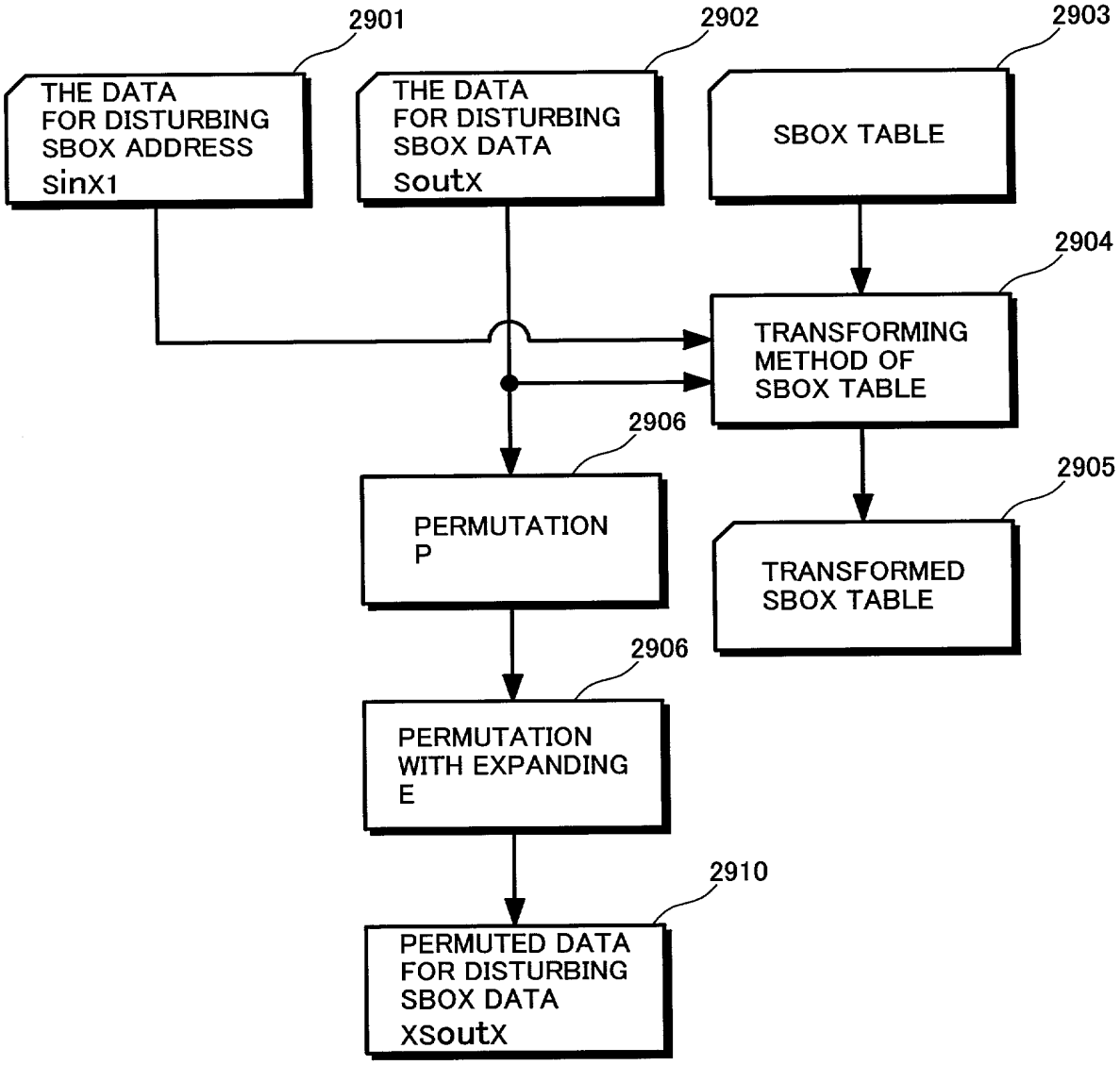
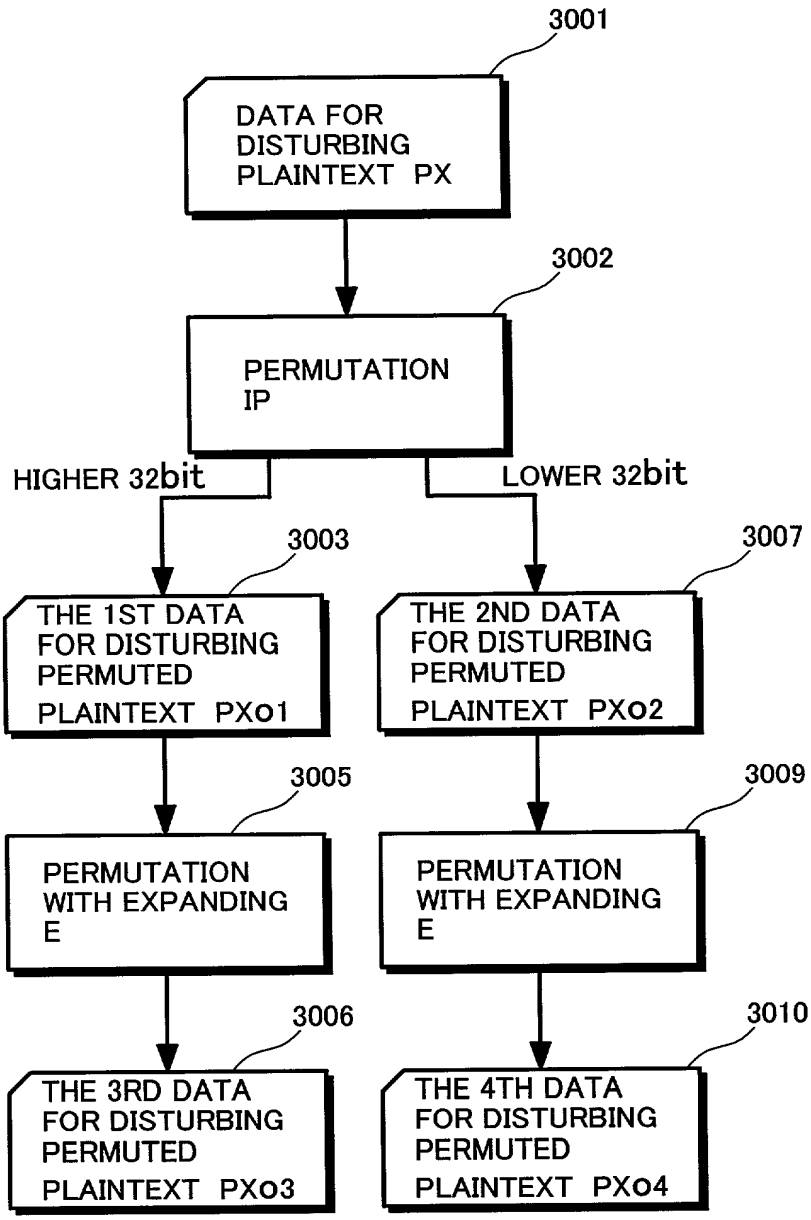

2901
THE DATA FOR DISTURBING SBOX ADDRESS SinX1
2902
THE DATA FOR DISTURBING SBOX DATA SoutX
2903
SBOX TABLE
2904
TRANSFORMING METHOD OF SBOX TABLE
2905
TRANSFORMED SBOX TABLE
2906
PERMUTATION P
2906
PERMUTATION WITH EXPANDING E
2910
PERMUTED DATA FOR DISTURBING SBOX DATA XSoutX

FIG. 30



US 6,985,582 B2

FIG. 31

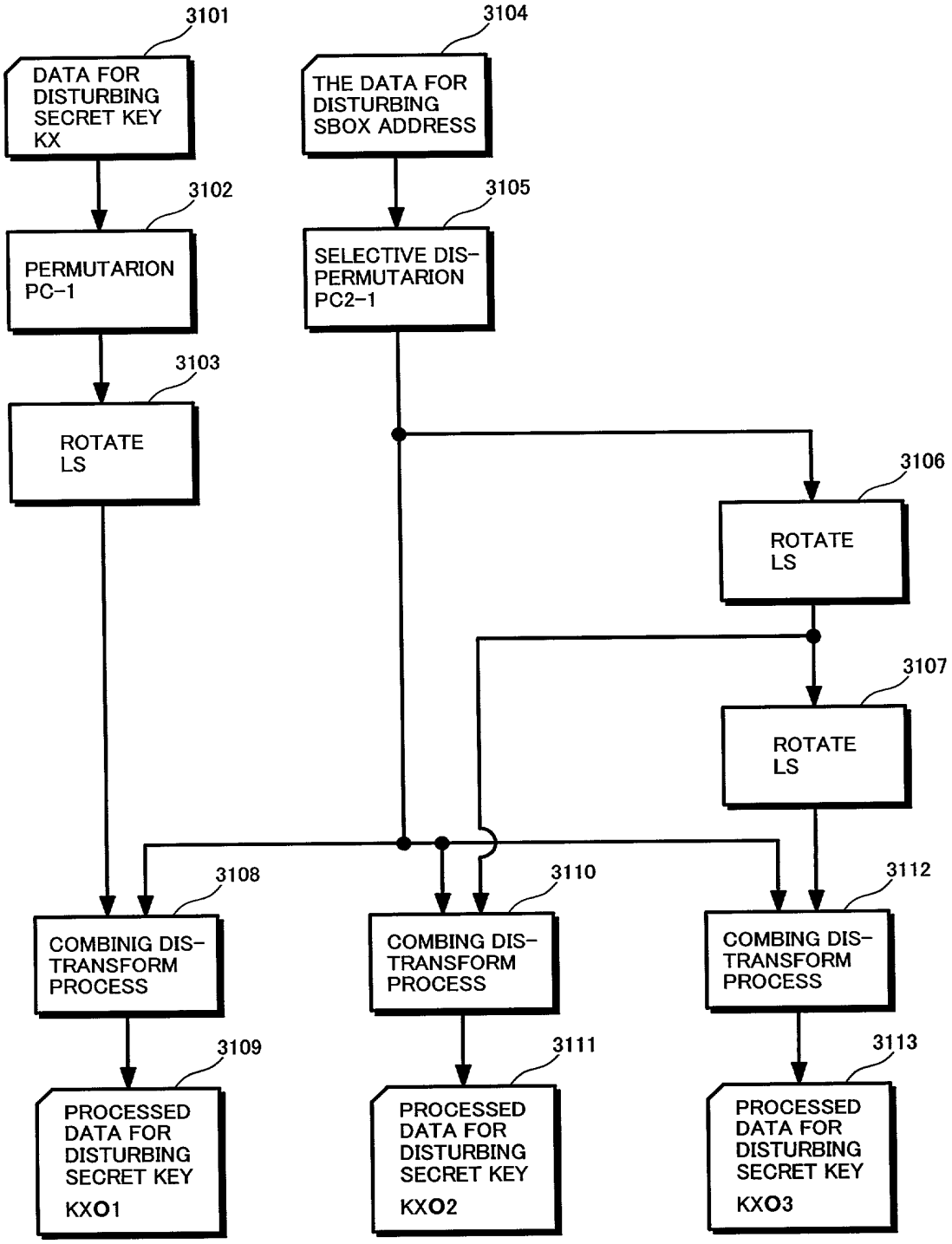

3101
DATA FOR DISTURBING SECRET KEY KX
3104
THE DATA FOR DISTURBING SBOX ADDRESS
3102
PERMUTARION PC-1
3105
SELECTIVE DIS-PERMUTARION PC2-1
3103
ROTATE LS
3106
ROTATE LS
3107
ROTATE LS
3108
COMBINIG DIS-TRANSFORM PROCESS
3110
COMBING DIS-TRANSFORM PROCESS
3112
COMBING DIS-TRANSFORM PROCESS
3109
PROCESSED DATA FOR DISTURBING SECRET KEY KXO1
3111
PROCESSED DATA FOR DISTURBING SECRET KEY KXO2
3113
PROCESSED DATA FOR DISTURBING SECRET KEY KXO3

FIG. 32

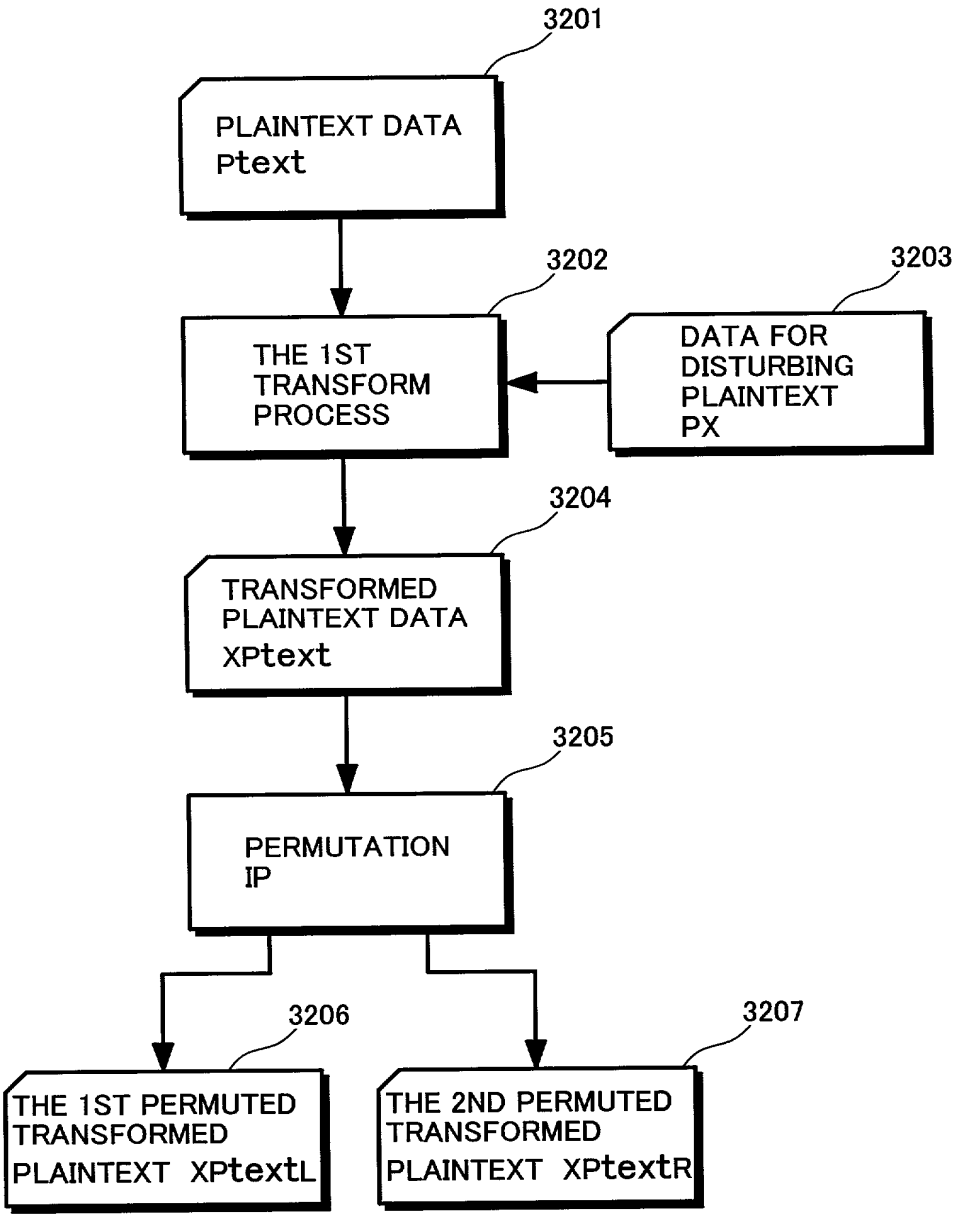

3201
PLAINTEXT DATA
Ptext
3202
THE 1ST
TRANSFORM
PROCESS
3203
DATA FOR
DISTURBING
PLAINTEXT
PX
3204
TRANSFORMED
PLAINTEXT DATA
XPtext
3205
PERMUTATION
IP
3206
THE 1ST PERMUTED
TRANSFORMED
PLAINTEXT XPtextL
3207
THE 2ND PERMUTED
TRANSFORMED
PLAINTEXT XPtextR

FIG. 33

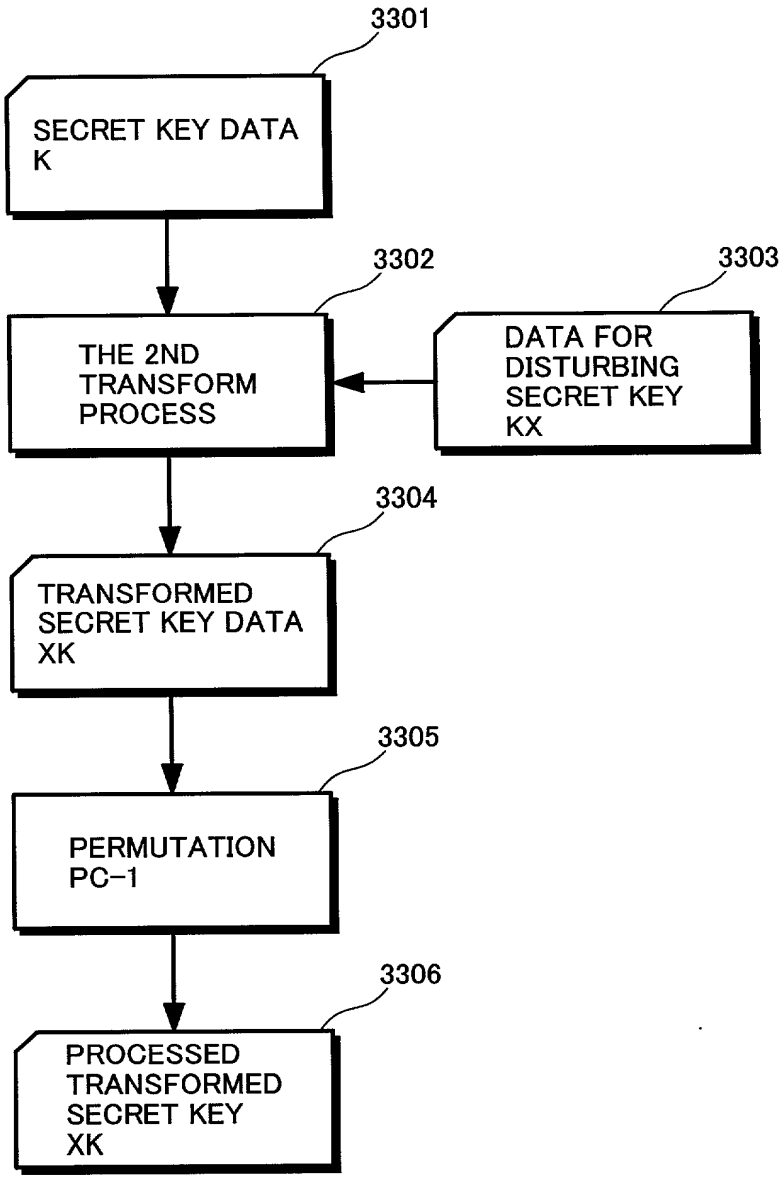

3301
SECRET KEY DATA K
3302
THE 2ND TRANSFORM PROCESS
3303
DATA FOR DISTURBING SECRET KEY KX
3304
TRANSFORMED SECRET KEY DATA XK
3305
PERMUTATION PC-1
3306
PROCESSED TRANSFORMED SECRET KEY XK

FIG. 34

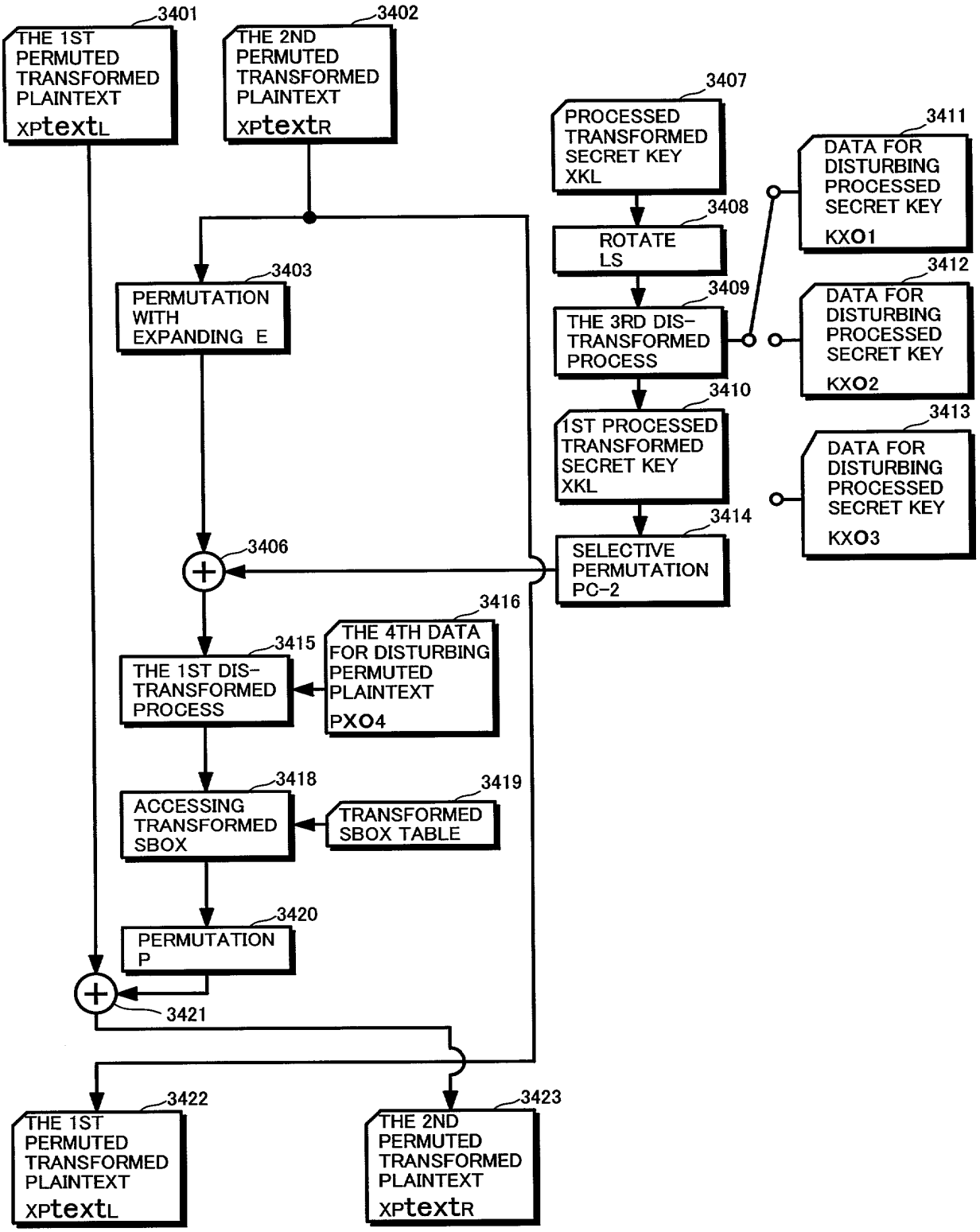

3401
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3402
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3403
PERMUTATION WITH EXPANDING E
3406
3407
PROCESSED TRANSFORMED SECRET KEY
XKL
3408
ROTATE LS
3409
THE 3RD DIS-TRANSFORMED PROCESS
3410
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3411
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO1
3412
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3413
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
3414
SELECTIVE PERMUTATION PC-2
3415
THE 1ST DIS-TRANSFORMED PROCESS
3416
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO4
3418
ACCESSING TRANSFORMED SBOX
3419
TRANSFORMED SBOX TABLE
3420
PERMUTATION P
3421
3422
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3423
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 35

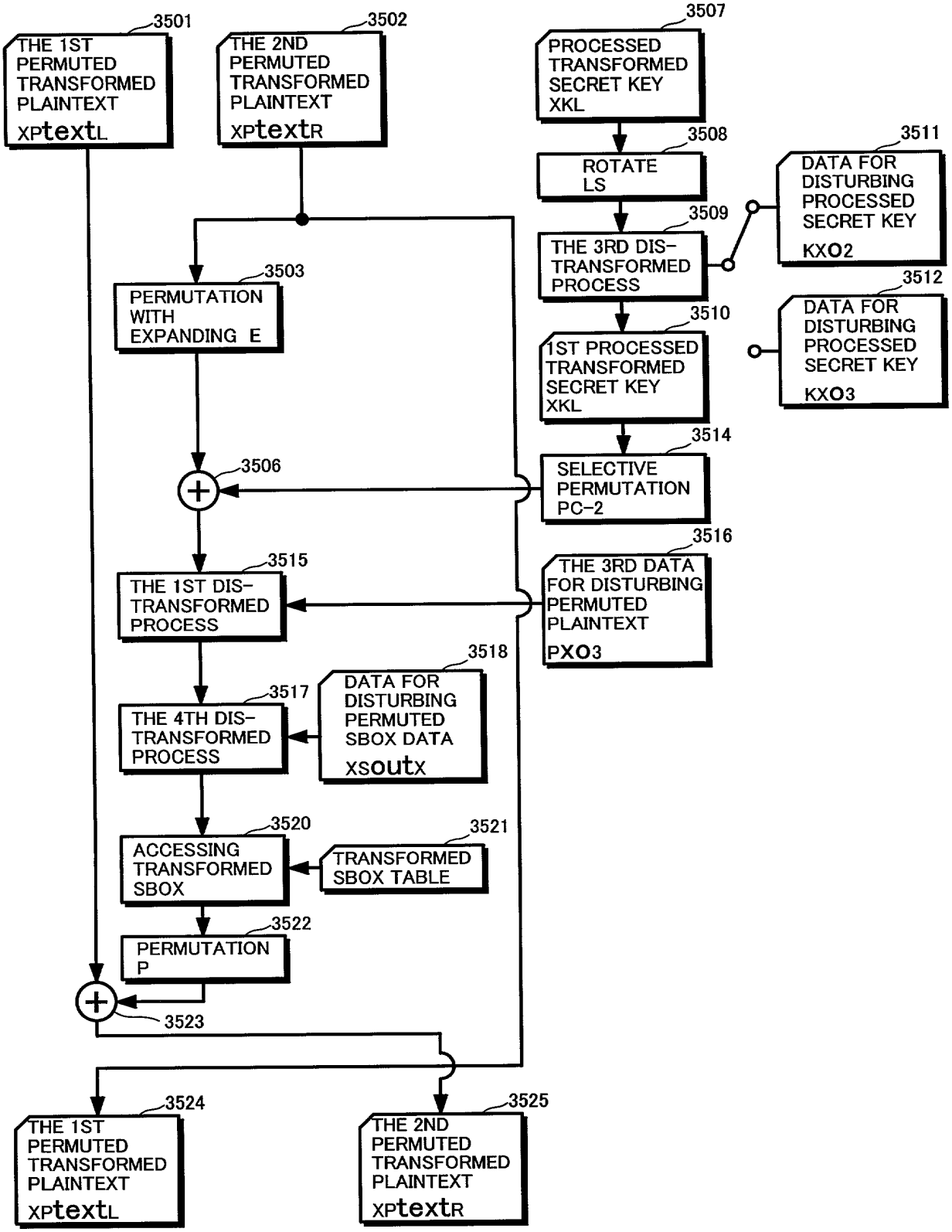

3501
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3502
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3507
PROCESSED TRANSFORMED SECRET KEY
XKL
3508
ROTATE LS
3511
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3509
THE 3RD DIS-TRANSFORMED PROCESS
3503
PERMUTATION WITH EXPANDING E
3512
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
3510
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3514
SELECTIVE PERMUTATION PC-2
3506
3516
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
3515
THE 1ST DIS-TRANSFORMED PROCESS
3518
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX
3517
THE 4TH DIS-TRANSFORMED PROCESS
3520
ACCESSING TRANSFORMED SBOX
3521
TRANSFORMED SBOX TABLE
3522
PERMUTATION P
3523
3524
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3525
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 36

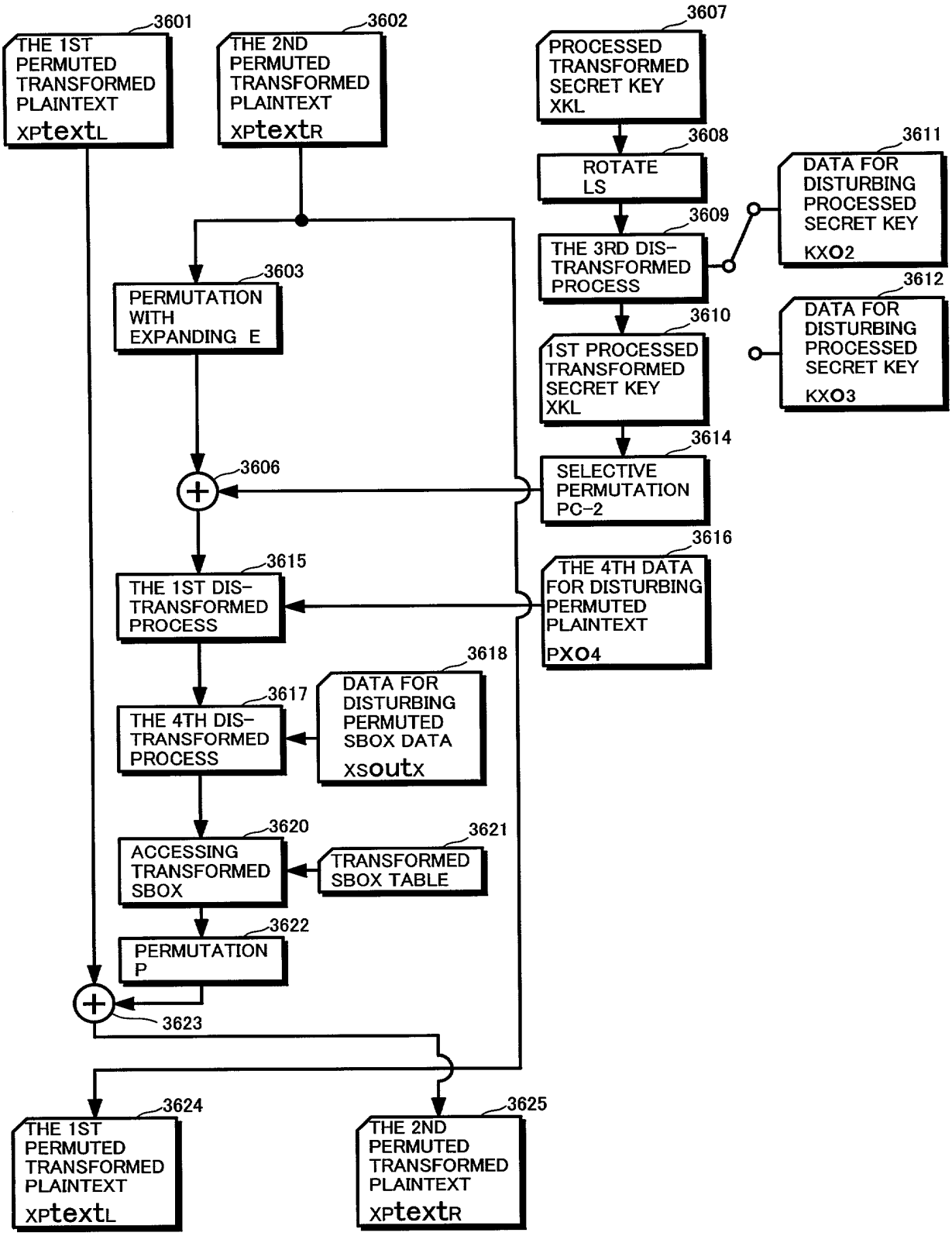

3601
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3602
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3607
PROCESSED TRANSFORMED SECRET KEY
XKL
3608
ROTATE LS
3611
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3609
THE 3RD DIS-TRANSFORMED PROCESS
3603
PERMUTATION WITH EXPANDING E
3612
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
3610
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3614
SELECTIVE PERMUTATION PC-2
3606
3616
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO4
3615
THE 1ST DIS-TRANSFORMED PROCESS
3618
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX
3617
THE 4TH DIS-TRANSFORMED PROCESS
3620
ACCESSING TRANSFORMED SBOX
3621
TRANSFORMED SBOX TABLE
3622
PERMUTATION P
3623
3624
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3625
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 37

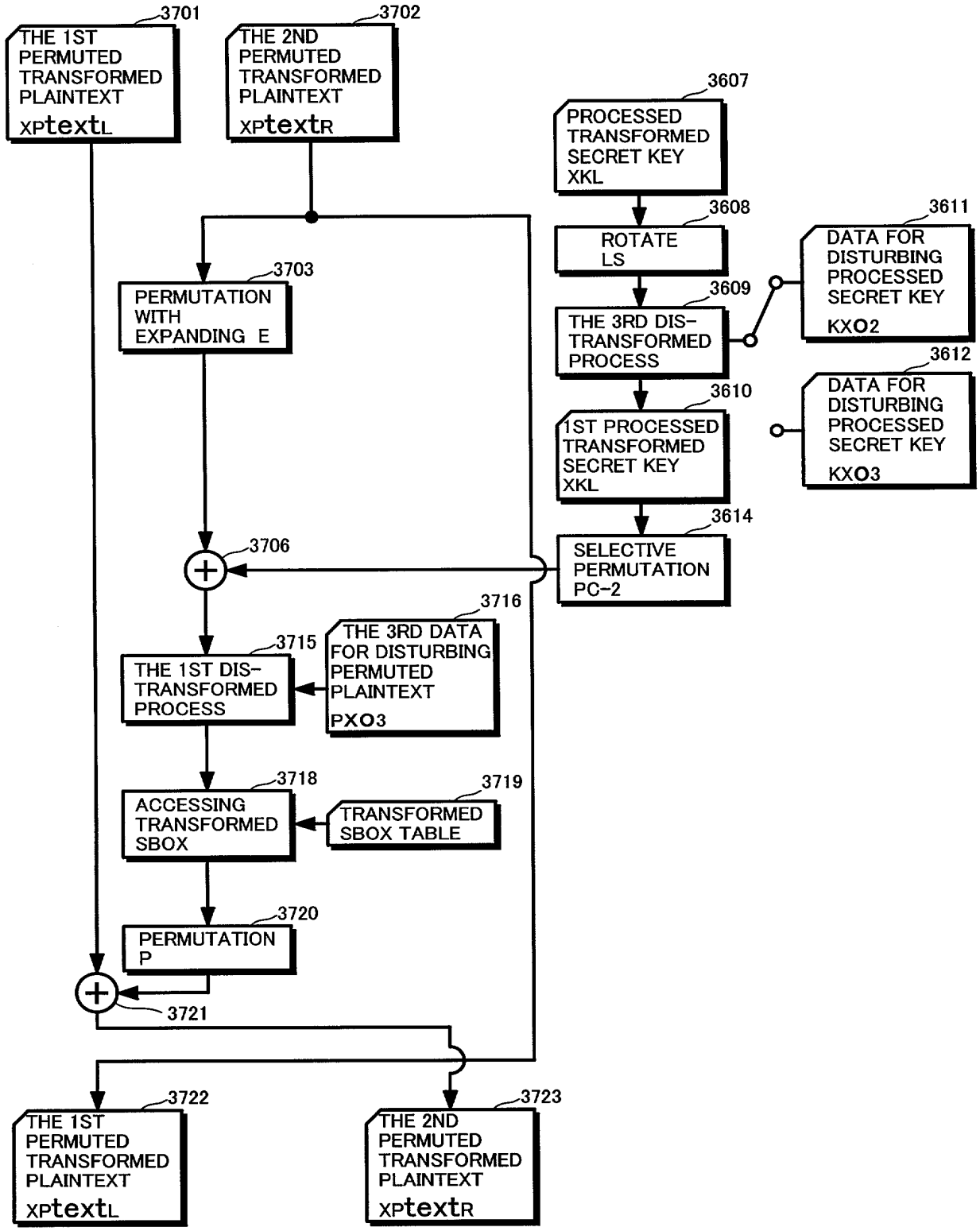

3701
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3702
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3607
PROCESSED TRANSFORMED SECRET KEY
XKL
3608
ROTATE LS
3611
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3609
THE 3RD DIS-TRANSFORMED PROCESS
3612
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
3610
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3614
SELECTIVE PERMUTATION PC-2
3703
PERMUTATION WITH EXPANDING E
3706
3716
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
3715
THE 1ST DIS-TRANSFORMED PROCESS
3718
ACCESSING TRANSFORMED SBOX
3719
TRANSFORMED SBOX TABLE
3720
PERMUTATION P
3721
3722
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3723
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 38

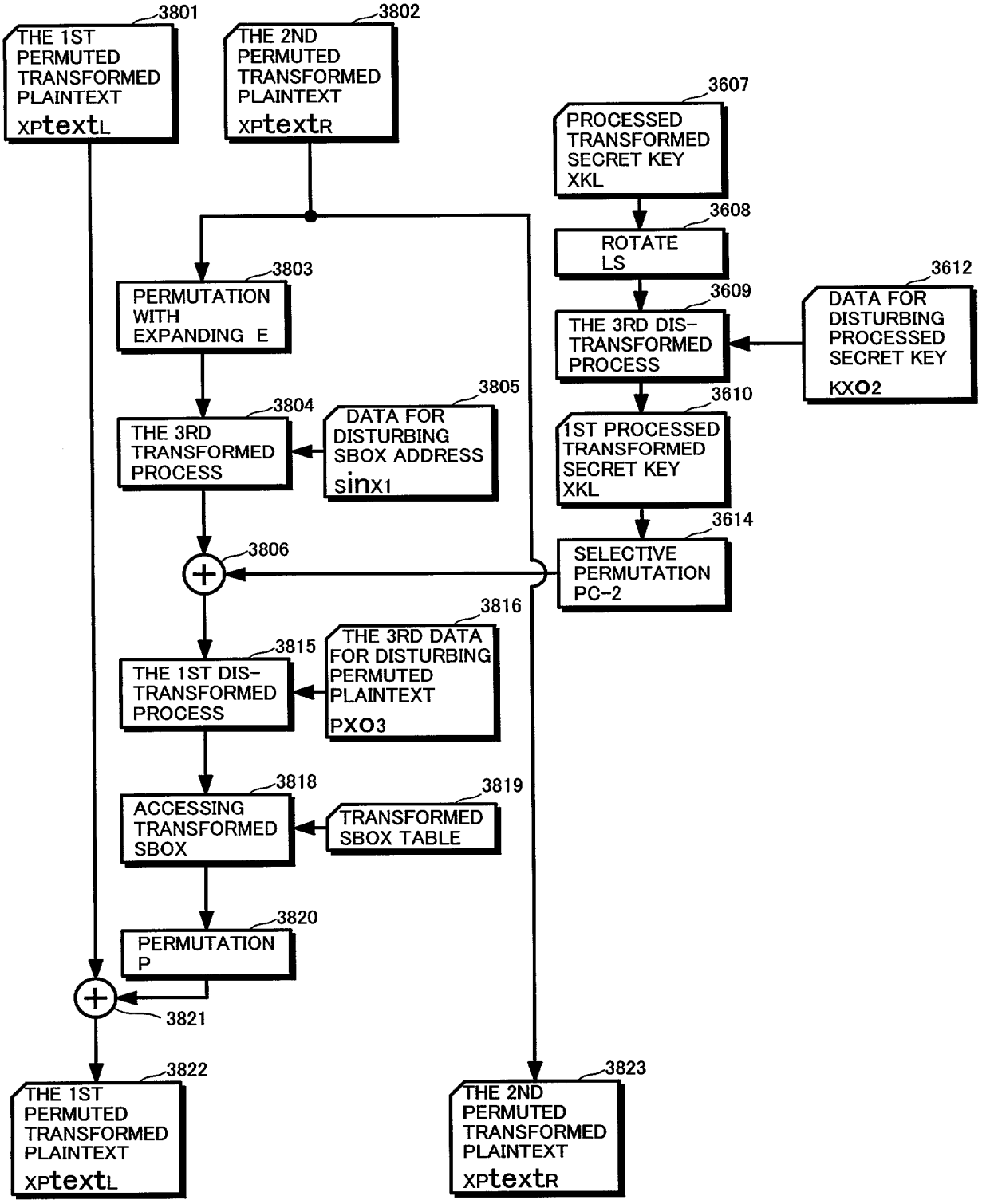

3801
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3802
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3607
PROCESSED TRANSFORMED SECRET KEY
XKL
3608
ROTATE LS
3612
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
3609
THE 3RD DIS-TRANSFORMED PROCESS
3803
PERMUTATION WITH EXPANDING E
3610
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
3805
DATA FOR DISTURBING SBOX ADDRESS
sinX1
3804
THE 3RD TRANSFORMED PROCESS
3614
SELECTIVE PERMUTATION PC-2
3806
3816
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
3815
THE 1ST DIS-TRANSFORMED PROCESS
3818
ACCESSING TRANSFORMED SBOX
3819
TRANSFORMED SBOX TABLE
3820
PERMUTATION P
3821
3822
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3823
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 39

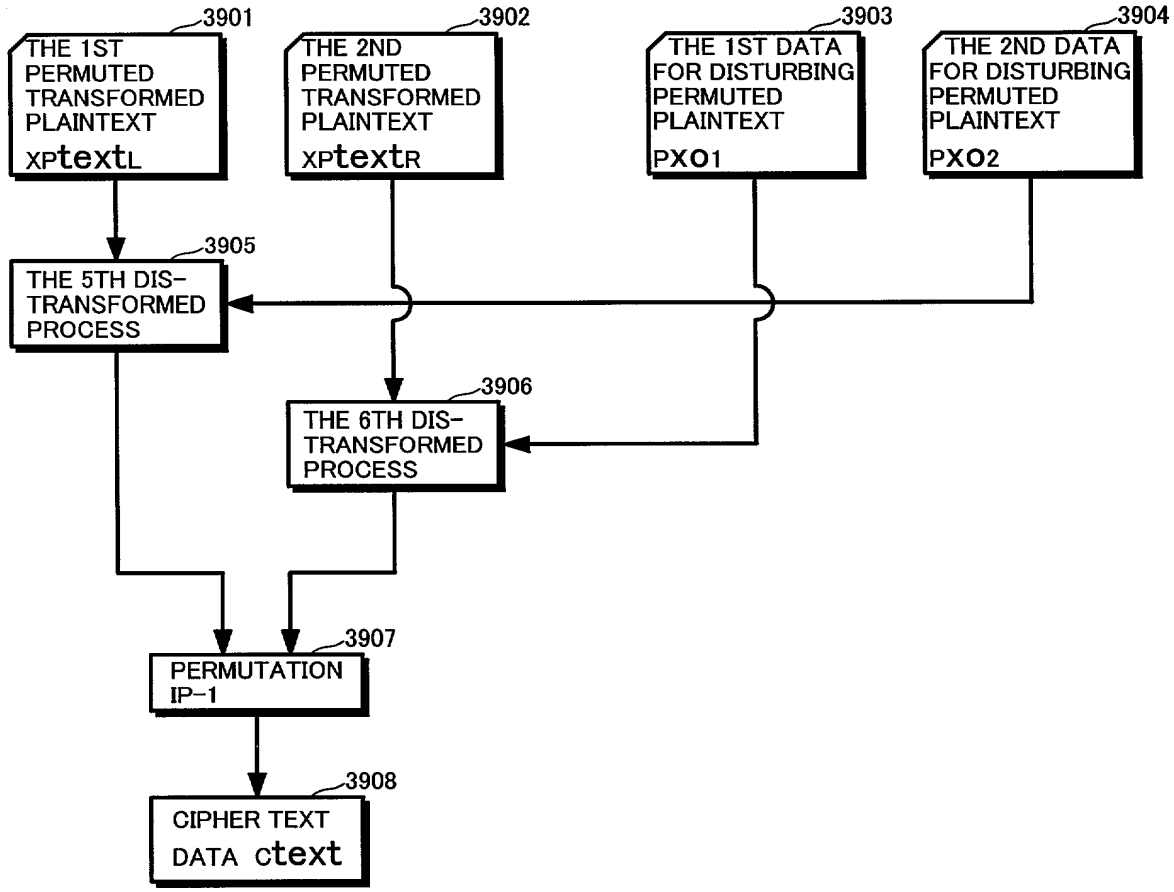

3901
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
3902
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
3903
THE 1ST DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO1
3904
THE 2ND DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO2
3905
THE 5TH DIS-TRANSFORMED PROCESS
3906
THE 6TH DIS-TRANSFORMED PROCESS
3907
PERMUTATION IP-1
3908
CIPHER TEXT DATA Ctext

FIG. 40

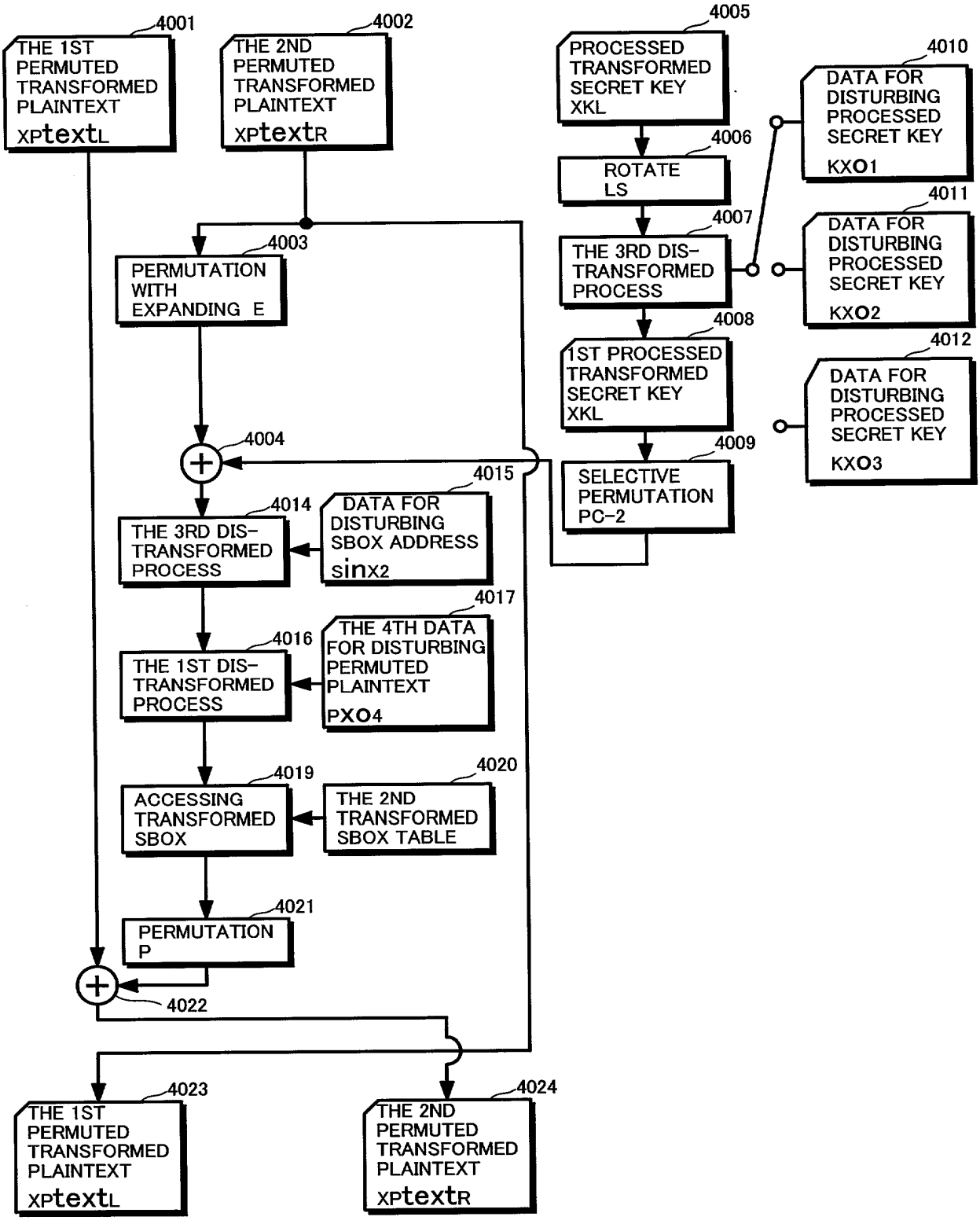

4001
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4002
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4003
PERMUTATION WITH EXPANDING E
4004
4005
PROCESSED TRANSFORMED SECRET KEY
XKL
4006
ROTATE LS
4007
THE 3RD DIS-TRANSFORMED PROCESS
4008
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
4009
SELECTIVE PERMUTATION PC-2
4010
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO1
4011
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
4012
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
4014
THE 3RD DIS-TRANSFORMED PROCESS
4015
DATA FOR DISTURBING SBOX ADDRESS
sinX2
4016
THE 1ST DIS-TRANSFORMED PROCESS
4017
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO4
4019
ACCESSING TRANSFORMED SBOX
4020
THE 2ND TRANSFORMED SBOX TABLE
4021
PERMUTATION P
4022
4023
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4024
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 41

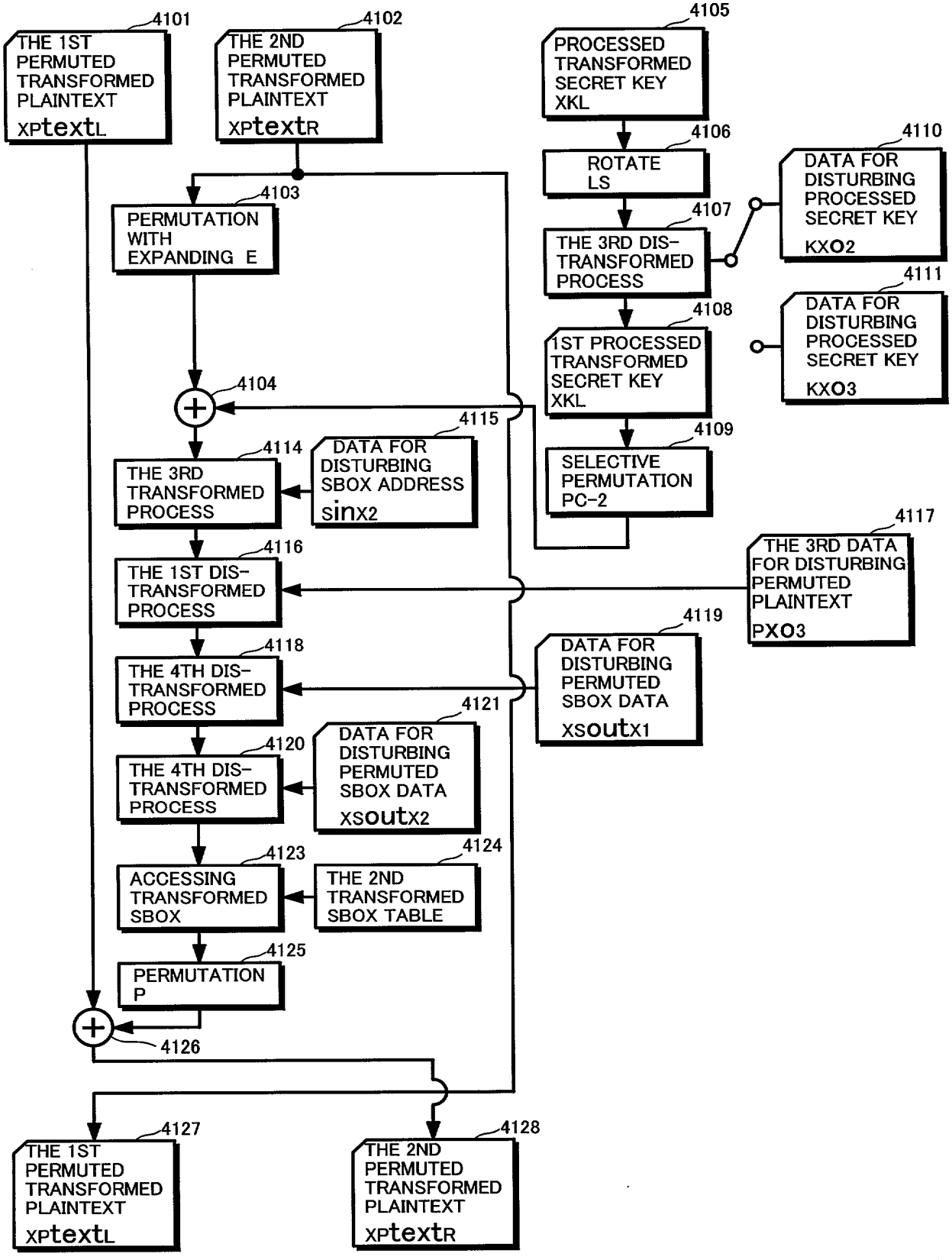

4101
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4102
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4103
PERMUTATION WITH EXPANDING E
4104
4105
PROCESSED TRANSFORMED SECRET KEY
XKL
4106
ROTATE LS
4107
THE 3RD DIS-TRANSFORMED PROCESS
4108
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
4109
SELECTIVE PERMUTATION PC-2
4110
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
4111
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
4114
THE 3RD TRANSFORMED PROCESS
4115
DATA FOR DISTURBING SBOX ADDRESS
sinX2
4116
THE 1ST DIS-TRANSFORMED PROCESS
4117
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
4118
THE 4TH DIS-TRANSFORMED PROCESS
4119
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX1
4120
THE 4TH DIS-TRANSFORMED PROCESS
4121
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX2
4123
ACCESSING TRANSFORMED SBOX
4124
THE 2ND TRANSFORMED SBOX TABLE
4125
PERMUTATION P
4126
4127
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4128
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 42

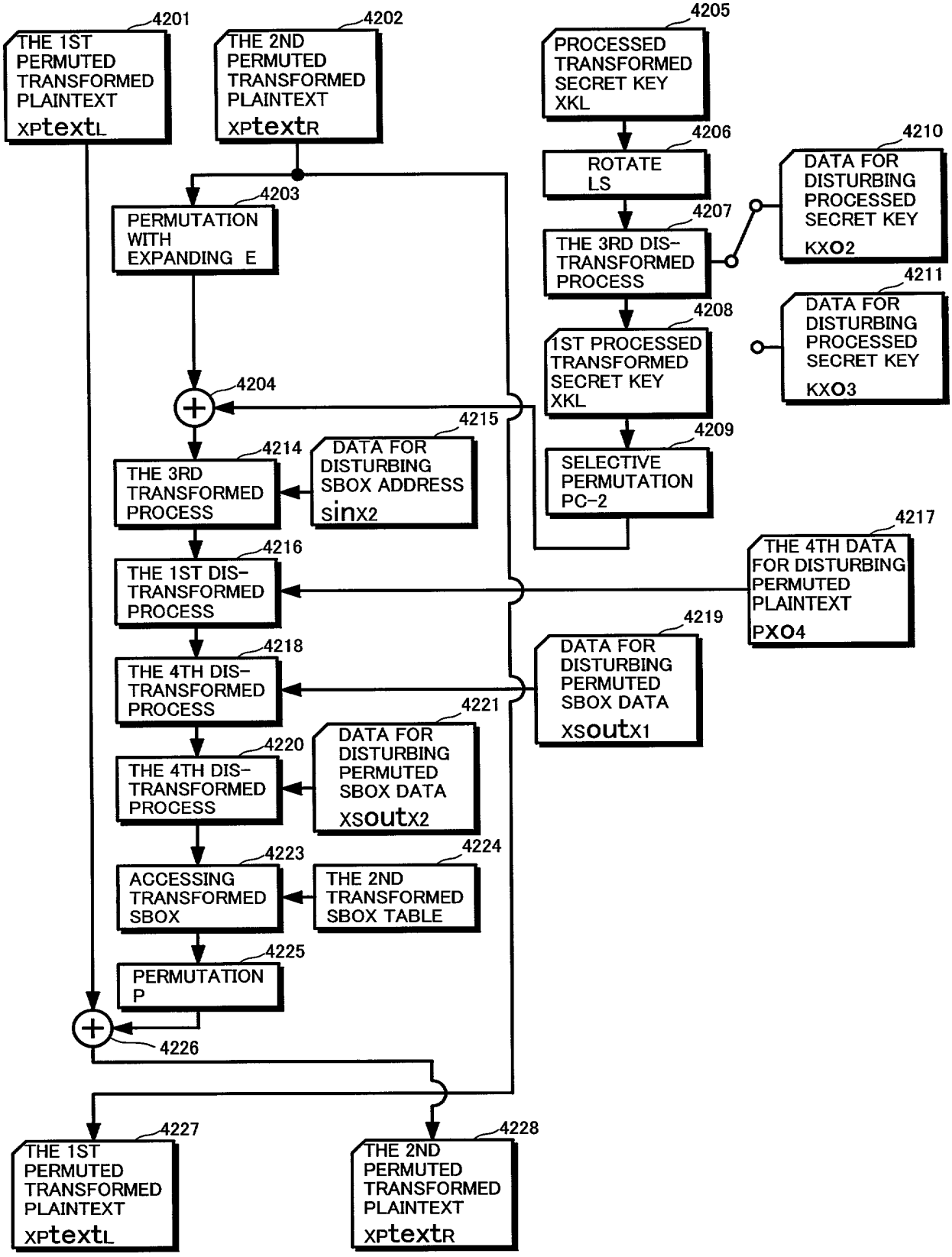

4201
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4202
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4205
PROCESSED TRANSFORMED SECRET KEY
XKL
4206
ROTATE LS
4210
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
4203
PERMUTATION WITH EXPANDING E
4207
THE 3RD DIS-TRANSFORMED PROCESS
4211
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
4208
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
4204
4215
4214
DATA FOR DISTURBING SBOX ADDRESS
sinX2
THE 3RD TRANSFORMED PROCESS
4209
SELECTIVE PERMUTATION PC-2
4217
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO4
4216
THE 1ST DIS-TRANSFORMED PROCESS
4219
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX1
4218
THE 4TH DIS-TRANSFORMED PROCESS
4221
DATA FOR DISTURBING PERMUTED SBOX DATA
XSoutX2
4220
THE 4TH DIS-TRANSFORMED PROCESS
4223
ACCESSING TRANSFORMED SBOX
4224
THE 2ND TRANSFORMED SBOX TABLE
4225
PERMUTATION P
4226
4227
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4228
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 43

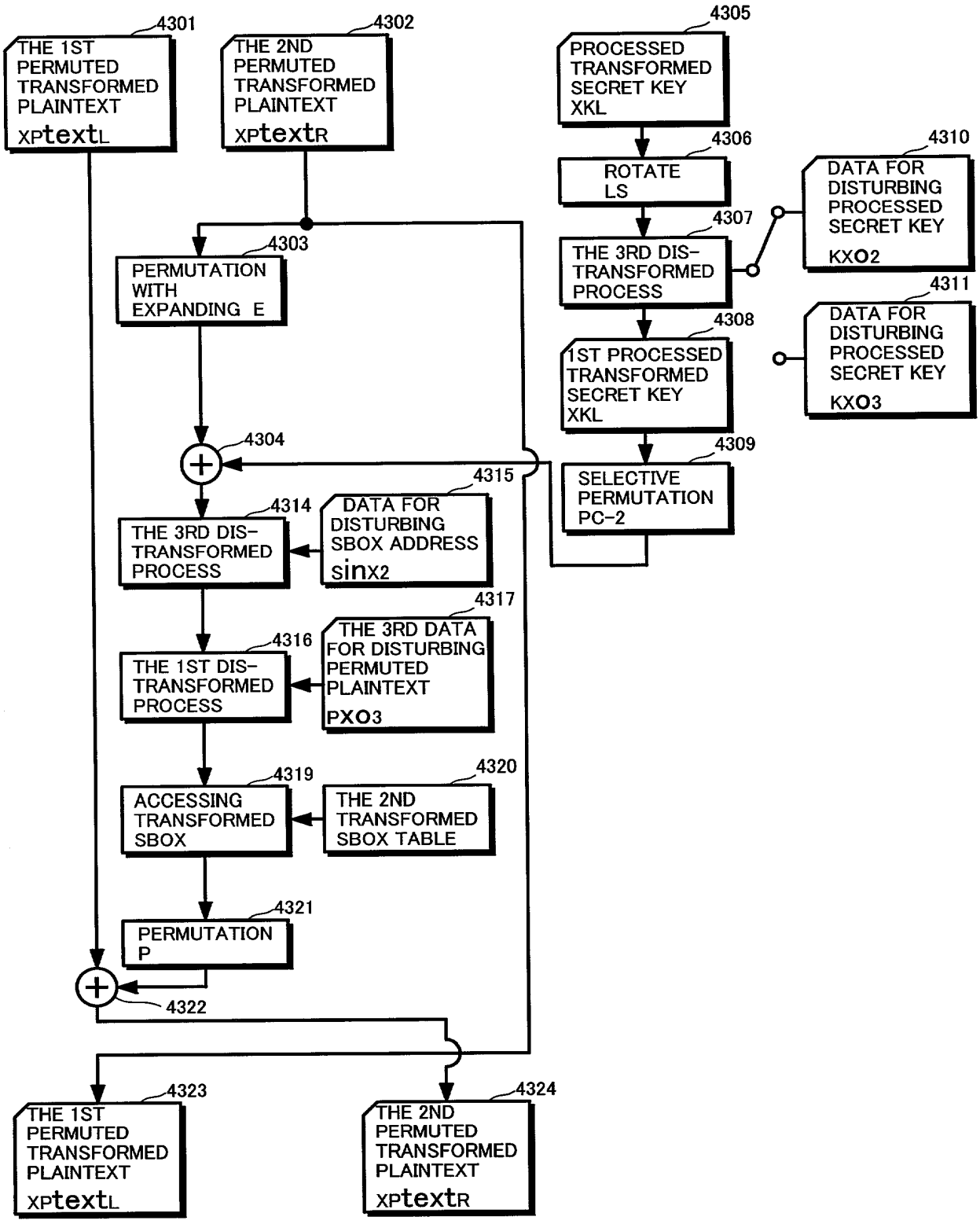

4301
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4302
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4303
PERMUTATION WITH EXPANDING E
4304
4305
PROCESSED TRANSFORMED SECRET KEY
XKL
4306
ROTATE LS
4307
THE 3RD DIS-TRANSFORMED PROCESS
4308
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
4309
SELECTIVE PERMUTATION PC-2
4310
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
4311
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
4314
THE 3RD DIS-TRANSFORMED PROCESS
4315
DATA FOR DISTURBING SBOX ADDRESS
sinX2
4316
THE 1ST DIS-TRANSFORMED PROCESS
4317
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
4319
ACCESSING TRANSFORMED SBOX
4320
THE 2ND TRANSFORMED SBOX TABLE
4321
PERMUTATION P
4322
4323
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4324
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 44

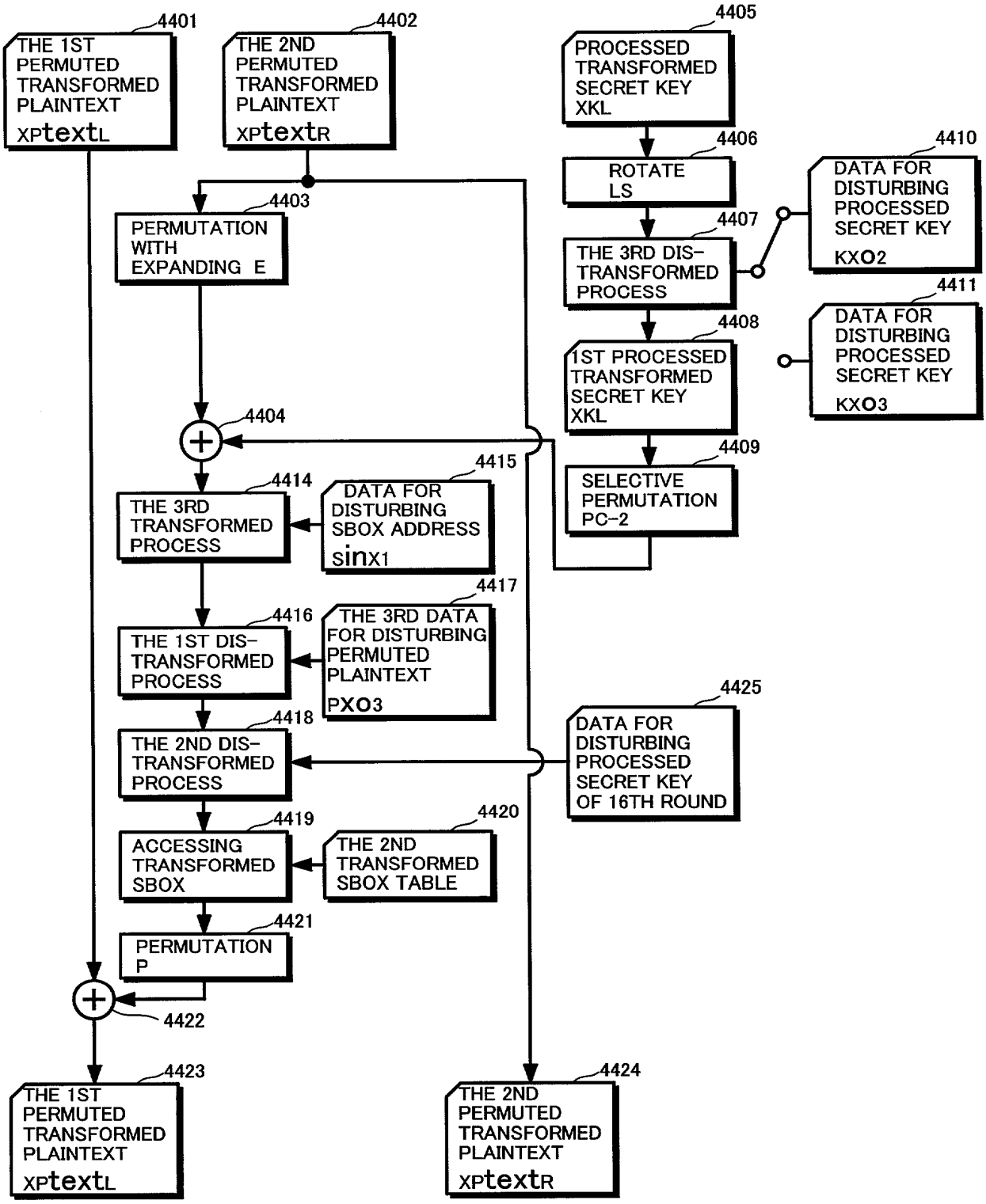

4401
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4402
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4403
PERMUTATION WITH EXPANDING E
4404
4405
PROCESSED TRANSFORMED SECRET KEY
XKL
4406
ROTATE LS
4407
THE 3RD DIS-TRANSFORMED PROCESS
4408
1ST PROCESSED TRANSFORMED SECRET KEY
XKL
4409
SELECTIVE PERMUTATION PC-2
4410
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO2
4411
DATA FOR DISTURBING PROCESSED SECRET KEY
KXO3
4414
THE 3RD TRANSFORMED PROCESS
4415
DATA FOR DISTURBING SBOX ADDRESS
sinX1
4416
THE 1ST DIS-TRANSFORMED PROCESS
4417
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT
PXO3
4418
THE 2ND DIS-TRANSFORMED PROCESS
4419
ACCESSING TRANSFORMED SBOX
4420
THE 2ND TRANSFORMED SBOX TABLE
4421
PERMUTATION P
4422
4423
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
4424
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR
4425
DATA FOR DISTURBING PROCESSED SECRET KEY OF 16TH ROUND

FIG. 45

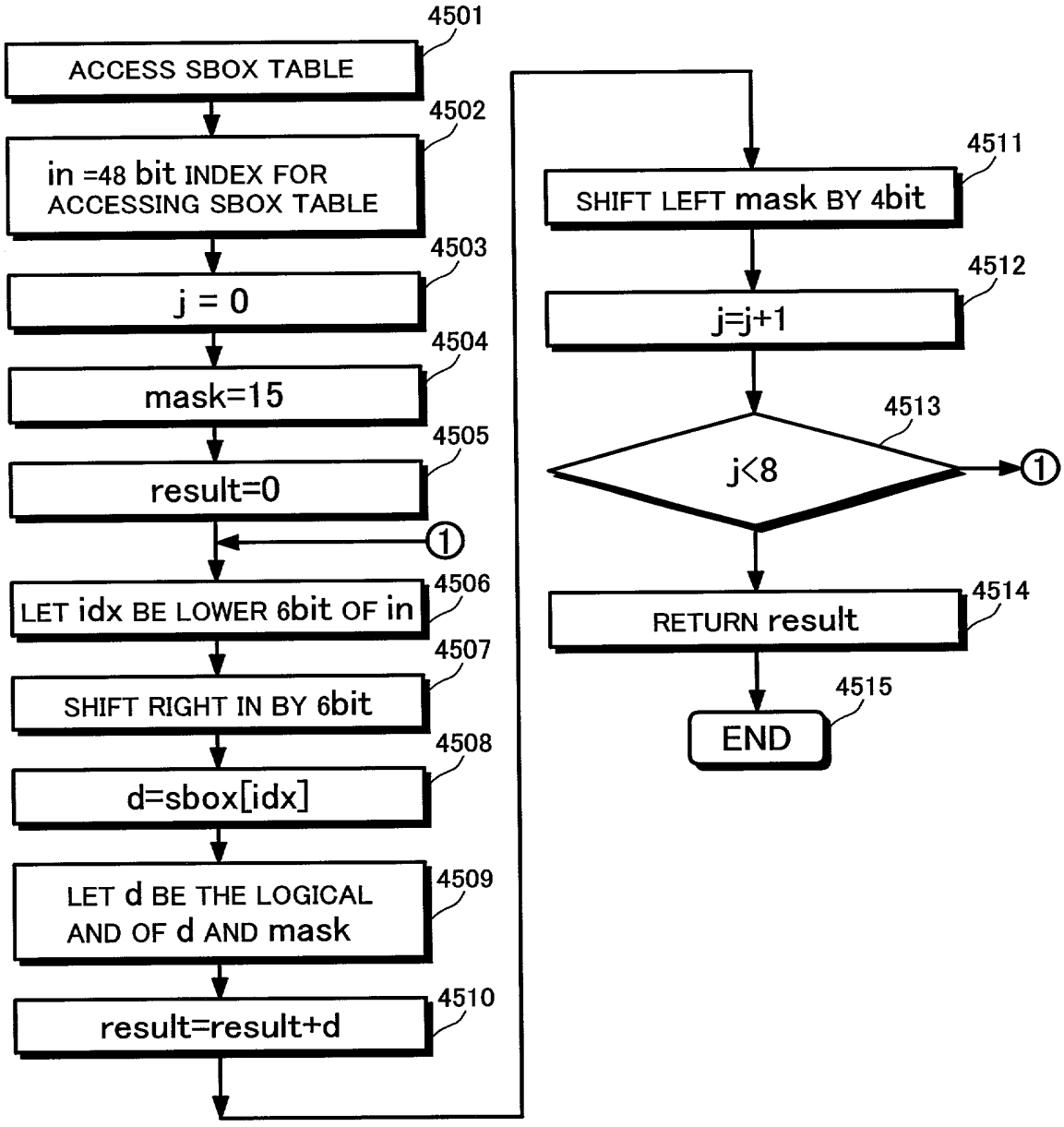

4501
ACCESS SBOX TABLE
4502
in =48 bit INDEX FOR ACCESSING SBOX TABLE
4503
j = 0
4504
mask=15
4505
result=0
①
4506
LET idx BE LOWER 6bit OF in
4507
SHIFT RIGHT IN BY 6bit
4508
d=sbox[idx]
4509
LET d BE THE LOGICAL AND OF d AND mask
4510
result=result+d
4511
SHIFT LEFT mask BY 4bit
4512
j=j+1
4513
j<8
①
4514
RETURN result
4515
END

FIG. 46

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0XEFA72CAD	16	0X3911803A	32	0X40DA4917	48	0XF5BFF7A0
1	0X03DDEAD1	17	0XAC2456EC	33	0XFD13B462	49	0X5B496B9F
2	0X410DC1B2	18	0XA7D25DC9	34	0X1E662E4B	50	0XC81190F6
3	0XFD78BF0F	19	0X60870135	35	0XC8AF83B1	51	0XB6F4FE5C
4	0XD89E4A28	20	0X62C83393	36	0XE7491FB4	52	0X9C23C46A
5	0X740B24BD	21	0XC152FD56	37	0X8AD0C2DE	53	0X37E50109
6	0X1EE31FE4	22	0XCD75F47E	38	0X8B90B5D1	54	0X76CE5A8D
7	0X4795C278	23	0XBAECAECB	39	0X21067C87	55	0XEC3B97F0
8	0X266079F6	24	0X5CBBDE55	40	0XDA8CA2C9	56	0X3955610F
9	0XEF36474A	25	0X96C13020	41	0X436A1914	57	0XA0BCA6E3
10	0XFB36A20F	26	0X904C07A0	42	0X64FBD83C	58	0XA3A23D53
11	0X224F7C93	27	0X59BA9BFE	43	0X9F91E54A	59	0X05574025
12	0XB3F9B68B	28	0X0524E56C	44	0X2D377C7E	60	0X52E80B95
13	0XD860D917	29	0X3BFE8389	45	0X148D2FA8	61	0X6E225836
14	0X845A68D1	30	0X7A8F9817	46	0XB10D83E2	62	0X0F74E628
15	0X1EA315A4	31	0X85196862	47	0X7278DA7D	63	0XD9CE3DCB

FIG. 47

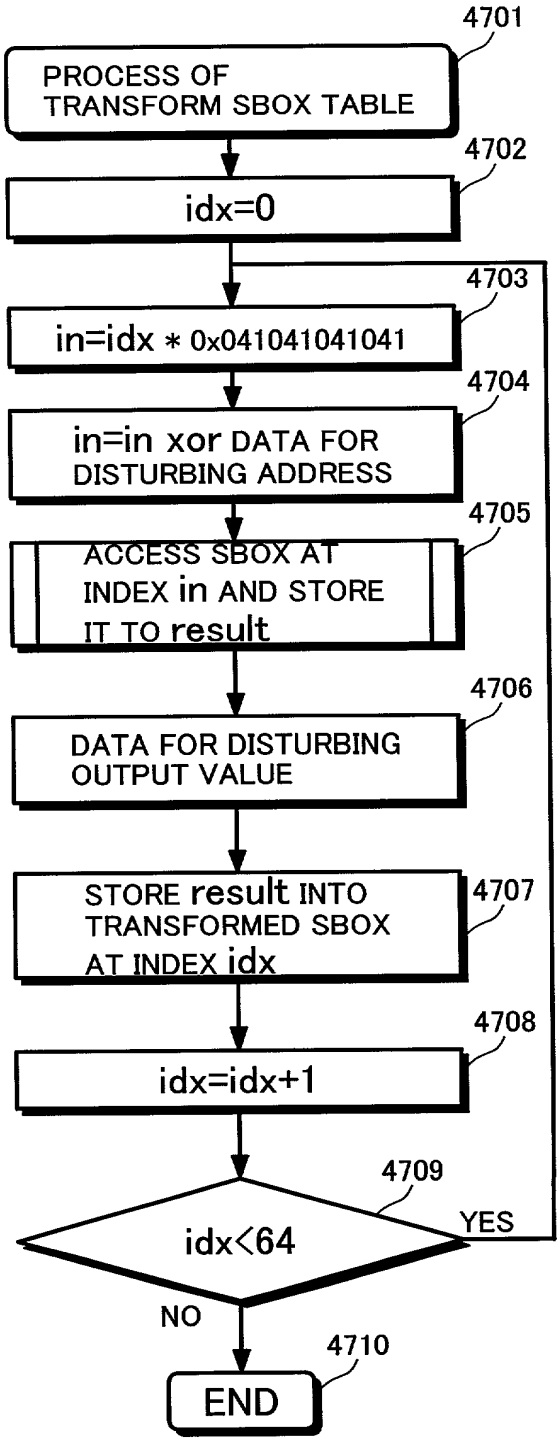

4701
PROCESS OF TRANSFORM SBOX TABLE
4702
idx=0
4703
in=idx * 0x041041041041
4704
in=in xor DATA FOR DISTURBING ADDRESS
4705
ACCESS SBOX AT INDEX in AND STORE IT TO result
4706
DATA FOR DISTURBING OUTPUT VALUE
4707
STORE result INTO TRANSFORMED SBOX AT INDEX idx
4708
idx=idx+1
4709
idx<64
YES
NO
4710
END

FIG. 48

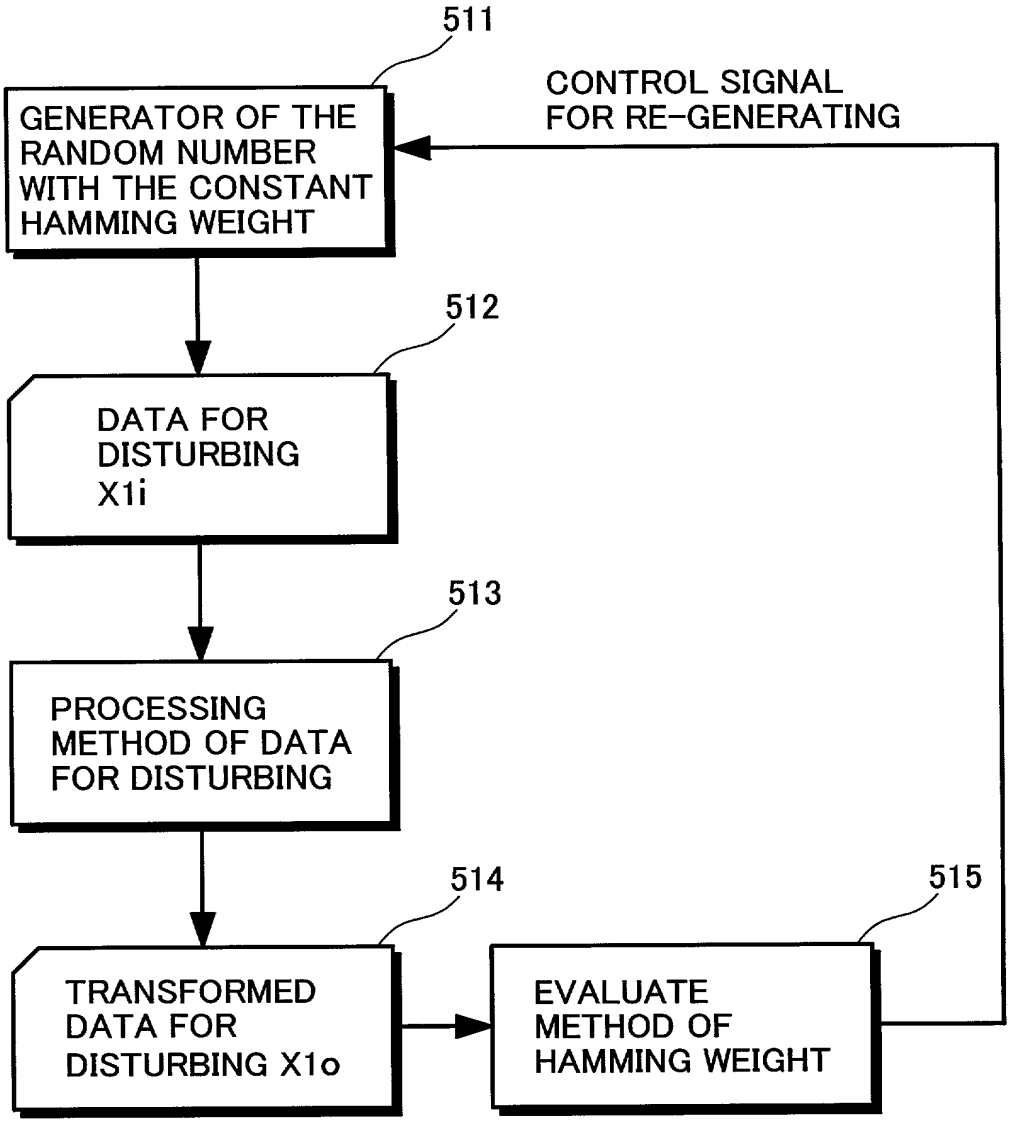

511
CONTROL SIGNAL FOR RE-GENERATING
GENERATOR OF THE RANDOM NUMBER WITH THE CONSTANT HAMMING WEIGHT
512
DATA FOR DISTURBING X1i
513
PROCESSING METHOD OF DATA FOR DISTURBING
514
515
TRANSFORMED DATA FOR DISTURBING X1o
EVALUATE METHOD OF HAMMING WEIGHT

FIG. 49

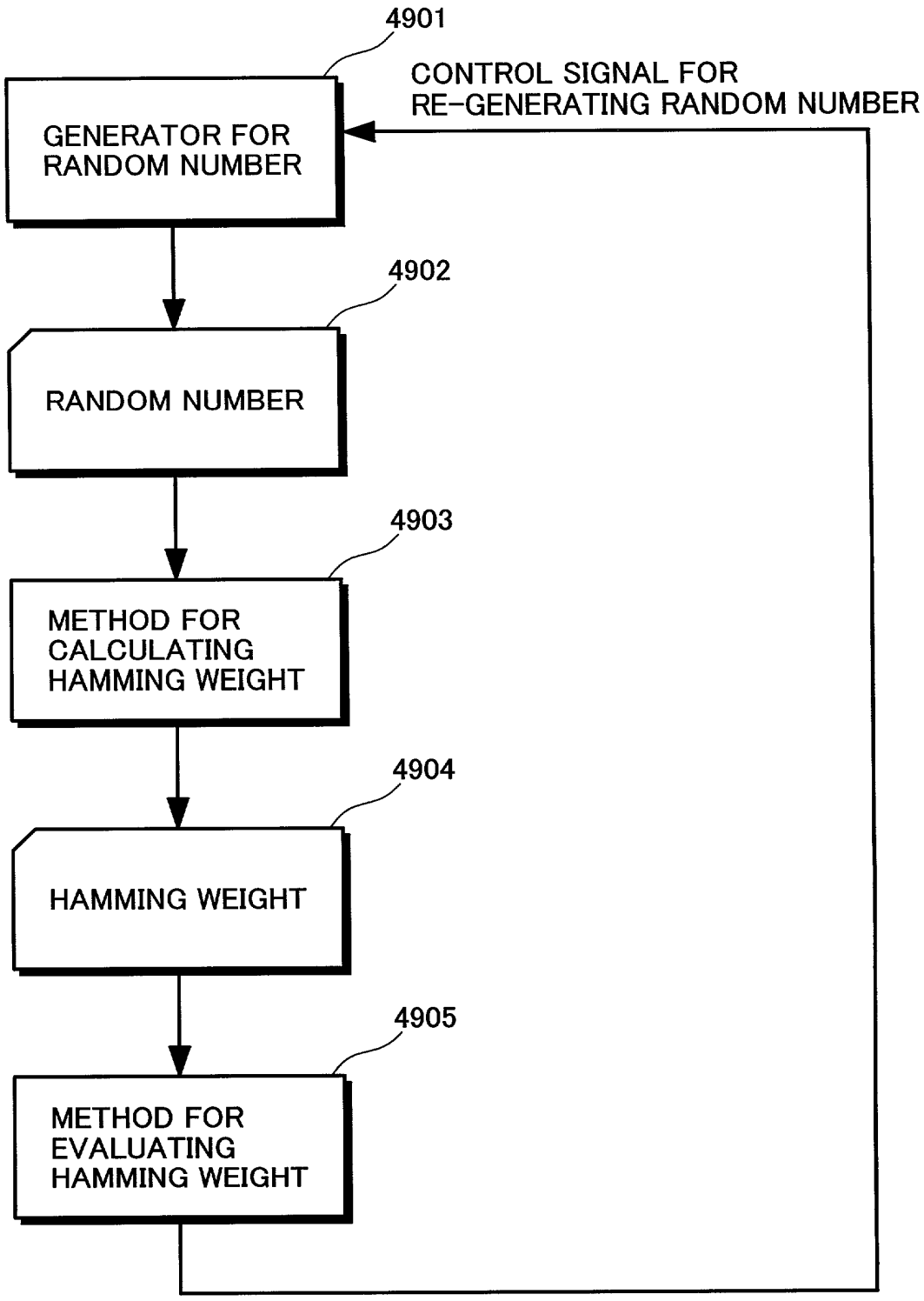

4901
CONTROL SIGNAL FOR
RE-GENERATING RANDOM NUMBER
GENERATOR FOR
RANDOM NUMBER
4902
RANDOM NUMBER
4903
METHOD FOR
CALCULATING
HAMMING WEIGHT
4904
HAMMING WEIGHT
4905
METHOD FOR
EVALUATING
HAMMING WEIGHT

FIG. 50

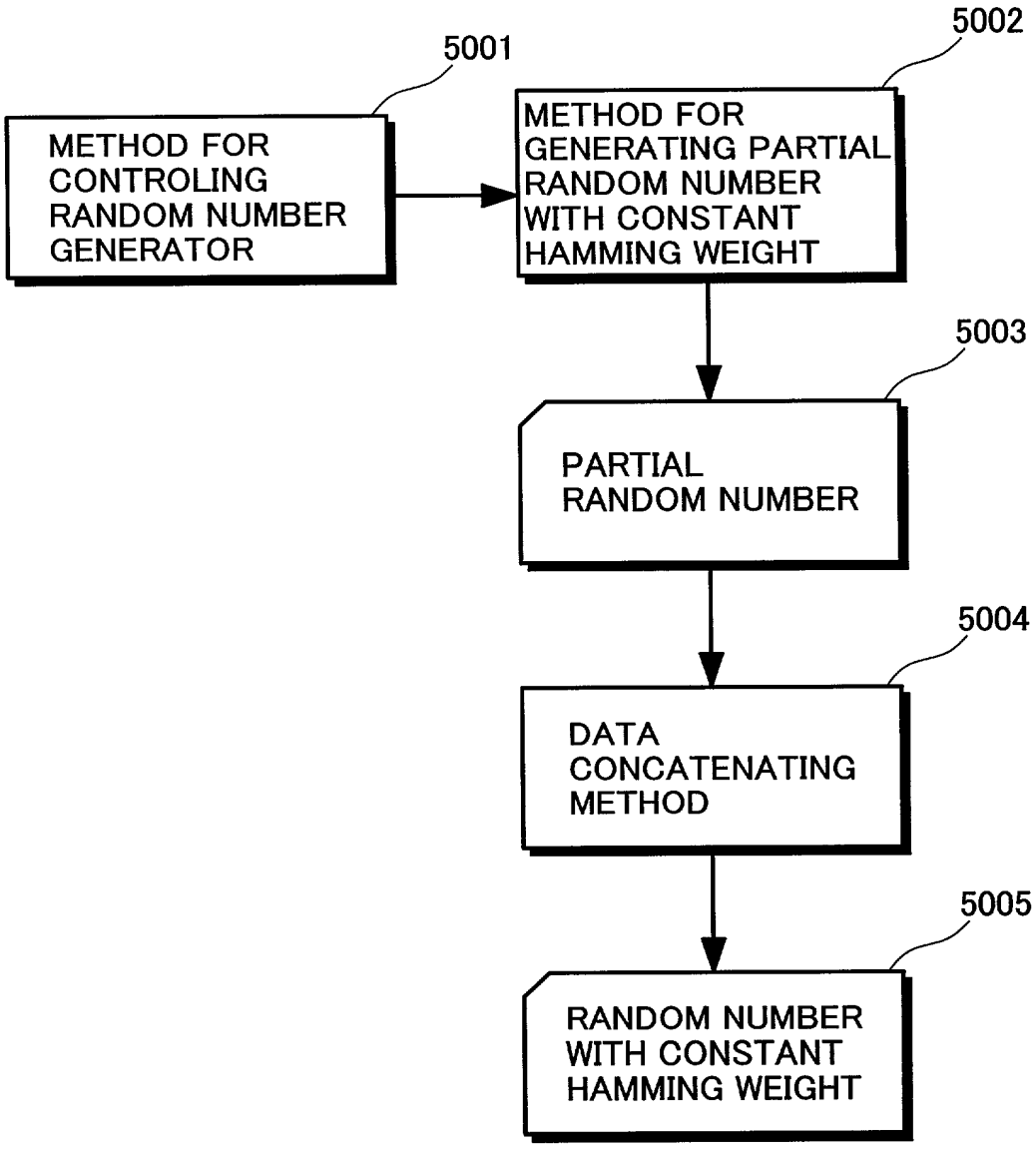
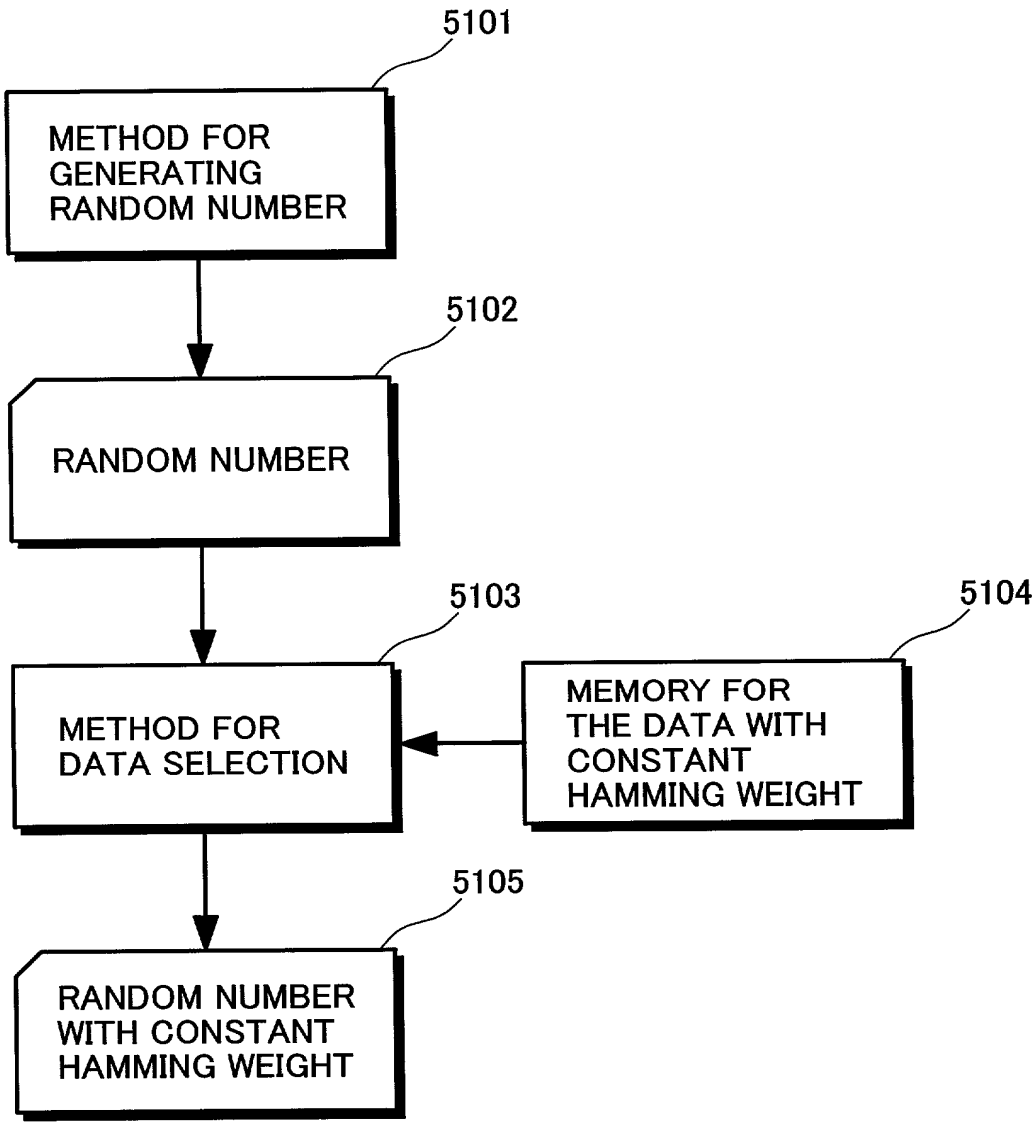

5001
METHOD FOR CONTROLING RANDOM NUMBER GENERATOR
5002
METHOD FOR GENERATING PARTIAL RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT
5003
PARTIAL RANDOM NUMBER
5004
DATA CONCATENATING METHOD
5005
RANDOM NUMBER WITH CONSTANT HAMMING WEIGHT

FIG. 51



05409852.082504

FIG. 52

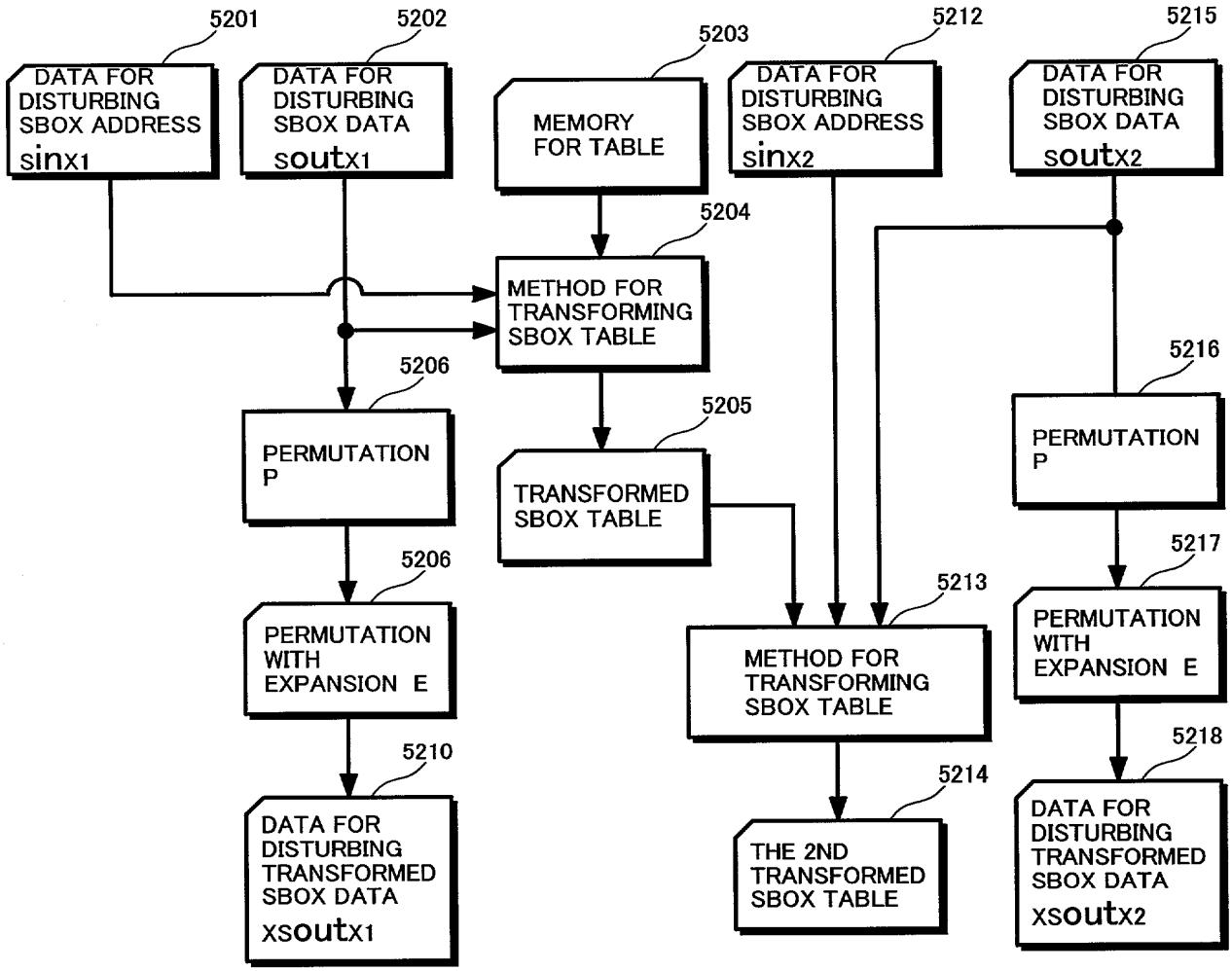

5201
DATA FOR DISTURBING SBOX ADDRESS
sinx1
5202
DATA FOR DISTURBING SBOX DATA
soutx1
5203
MEMORY FOR TABLE
5212
DATA FOR DISTURBING SBOX ADDRESS
sinx2
5215
DATA FOR DISTURBING SBOX DATA
soutx2
5204
METHOD FOR TRANSFORMING SBOX TABLE
5206
PERMUTATION P
5205
TRANSFORMED SBOX TABLE
5216
PERMUTATION P
5206
PERMUTATION WITH EXPANSION E
5213
METHOD FOR TRANSFORMING SBOX TABLE
5217
PERMUTATION WITH EXPANSION E
5210
DATA FOR DISTURBING TRANSFORMED SBOX DATA
xsoutx1
5214
THE 2ND TRANSFORMED SBOX TABLE
5218
DATA FOR DISTURBING TRANSFORMED SBOX DATA
xsoutx2

FIG. 53

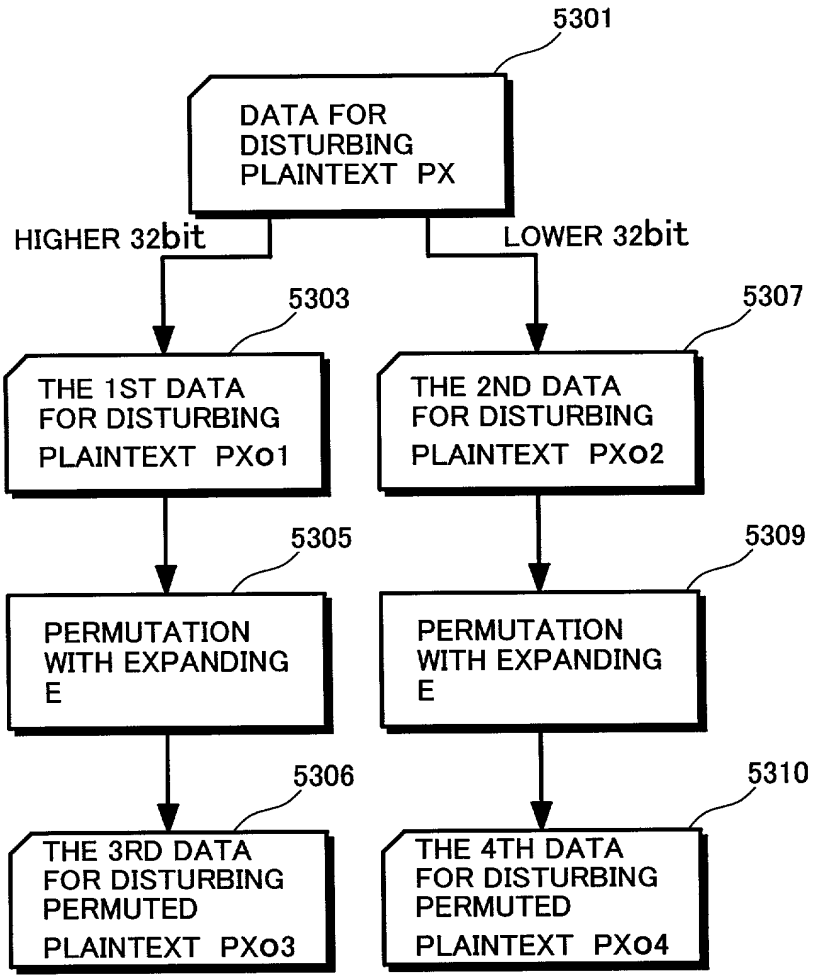

5301
DATA FOR DISTURBING PLAINTEXT PX
HIGHER 32bit
LOWER 32bit
5303
THE 1ST DATA FOR DISTURBING PLAINTEXT PXo1
5307
THE 2ND DATA FOR DISTURBING PLAINTEXT PXo2
5305
PERMUTATION WITH EXPANDING E
5309
PERMUTATION WITH EXPANDING E
5306
THE 3RD DATA FOR DISTURBING PERMUTED PLAINTEXT PXo3
5310
THE 4TH DATA FOR DISTURBING PERMUTED PLAINTEXT PXo4

FIG. 54

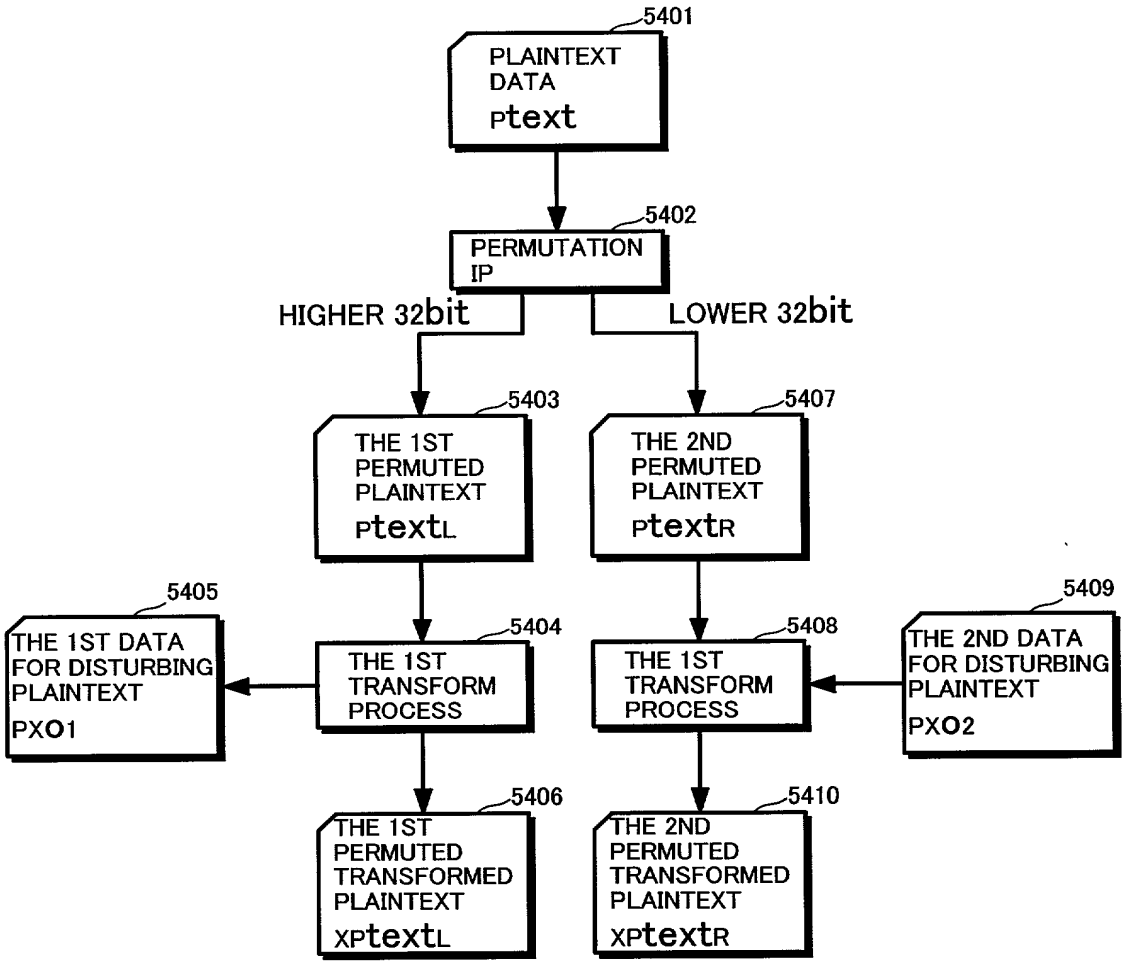

5401
PLAINTEXT DATA
Ptext
5402
PERMUTATION IP
HIGHER 32bit
LOWER 32bit
5403
THE 1ST PERMUTED PLAINTEXT
PtextL
5407
THE 2ND PERMUTED PLAINTEXT
PtextR
5405
THE 1ST DATA FOR DISTURBING PLAINTEXT
PXO1
5404
THE 1ST TRANSFORM PROCESS
5408
THE 1ST TRANSFORM PROCESS
5409
THE 2ND DATA FOR DISTURBING PLAINTEXT
PXO2
5406
THE 1ST PERMUTED TRANSFORMED PLAINTEXT
XPtextL
5410
THE 2ND PERMUTED TRANSFORMED PLAINTEXT
XPtextR

FIG. 55

IN THE CASE OF LEFT ROTATION

1201

X1i	X1o
0X55555555	0xaaaaaaaa
0X33333333	0X66666666
0X66666666	0XCCCCCCCC

FIG. 56

1501

THE 1ST DATA FOR DISTURBING
0X1C71C71C71C7
0X38E38E38E38E
0X34D34D34D34D
0X2CB2CB2CB2CB
0X38E38E38E38E

1502

THE 2ND DATA FOR DISTURBING
0X55555555
0XAAAAAAAA
0X0F0F0F0F
0X71717171
0X5A5A5A5A

FIG. 57

IN THE CASE OF
THE 1ST DATA FOR DISTURBING=0x1c71c71c71c7
THE 2ND DATA FOR DISTURBING=0x55555555

1507

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0XEFA72CAD	16	0X3911803A	32	0X40DA4917	48	0XF5BFF7A0
1	0X03DDEAD1	17	0XAC2456EC	33	0XFD13B462	49	0X5B496B9F
2	0X410DC1B2	18	0XA7D25DC9	34	0X1E662E4B	50	0XC81190F6
3	0XFD78BF0F	19	0X60870135	35	0XC8AF83B1	51	0XB6F4FE5C
4	0XD89E4A28	20	0X62C83393	36	0XE7491FB4	52	0X9C23C46A
5	0X740B24BD	21	0XC152FD56	37	0X8AD0C2DE	53	0X37E50109
6	0X1EE31FE4	22	0XCD75F47E	38	0X8B90B5D1	54	0X76CE5A8D
7	0X4795C278	23	0XBAECAECB	39	0X21067C87	55	0XEC3B97F0
8	0X266079F6	24	0X5CBBDE55	40	0XDA8CA2C9	56	0X3955610F
9	0XEF36474A	25	0X96C13020	41	0X436A1914	57	0XA0BCA6E3
10	0XFB36A20F	26	0X904C07A0	42	0X64FBD83C	58	0XA3A23D53
11	0X224F7C93	27	0X59BA9BFE	43	0X9F91E54A	59	0X05574025
12	0XB3F9B68B	28	0X0524E56C	44	0X2D377C7E	60	0X52E80B95
13	0XD860D917	29	0X3BFE8389	45	0X148D2FA8	61	0X6E225836
14	0X845A68D1	30	0X7A8F9817	46	0XB10D83E2	62	0X0F74E628
15	0X1EA315A4	31	0X85196862	47	0X7278DA7D	63	0XD9CE3DCB

1507

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0X12C0972D	16	0XEFB9FB9E	32	0X745329D2	48	0XB96EC2A5
1	0X4BB64AB1	17	0X9820A12B	33	0XDE05E084	49	0X239B0FD8
2	0X215E71E8	18	0X9407A803	34	0XDF85978B	50	0X62B0545C
3	0X8DCB1F7D	19	0X379D66C6	35	0X821C4AE1	51	0XC976913F
4	0XA82DEA5A	20	0X35D25460	36	0X9DFAD6E4	52	0XE3A1AB09
5	0X145894E7	21	0XF287089C	37	0X4B337B1E	53	0X9D44C5A3
6	0X5688BF84	22	0XF97103B9	38	0XA846E137	54	0X0E1C3ECA
7	0XBAF27918	23	0X6C44D56F	39	0X158F1C42	55	0XA0EAA2F5
8	0X4BF640F1	24	0XD04C3D37	40	0X272D8F28	56	0X8C9B689E
9	0XD10F3D84	25	0X2FDACE42	41	0XE458D6B7	57	0X5A21B37D
10	0X8D358C42	26	0X6EABD6DC	42	0X41D87AFD	58	0X3B770D63
11	0XE6ACE3DE	27	0X5071B039	43	0X7862292B	59	0X07BD5EC0
12	0X771A29C6	28	0X0CEFCEAB	44	0XCAC4B01F	60	0X50021570
13	0XAE63F75A	29	0XC51952F5	45	0X31AE8D69	61	0XF6F76806
14	0XBA63121F	30	0XC3946575	46	0X163F4C41	62	0XF5E9F3B6
15	0X73352CA3	31	0X09EE8B00	47	0X8FD9F79C	63	0X6C00345A

US 2006/0059204 A1 Mar. 16, 2006

FIG. 58

1602

INDEX	VALUE	INDEX	VALUE	INDEX	VALUE	INDEX	VALUE
0	0X12C0972D	16	0XEFB9FB9E	32	0X745329D2	48	0XB96EC2A5
1	0X4BB64AB1	17	0X9820A12B	33	0XDE05E084	49	0X239B0FD8
2	0X215E71E8	18	0X9407A803	34	0XDF85978B	50	0X62B0545C
3	0X8DCB1F7D	19	0X379D66C6	35	0X821C4AE1	51	0XC976913F
4	0XA82DEA5A	20	0X35D25460	36	0X9DFAD6E4	52	0XE3A1AB09
5	0X145894E7	21	0XF287089C	37	0X4B337B1E	53	0X9D44C5A3
6	0X5688BF84	22	0XF97103B9	38	0XA846E137	54	0X0E1C3ECA
7	0XBAF27918	23	0X6C44D56F	39	0X158F1C42	55	0XA0EAA2F5
8	0X4BF640F1	24	0XD04C3D37	40	0X272D8F28	56	0X8C9B689E
9	0XD10F3D84	25	0X2FDACE42	41	0XE458D6B7	57	0X5A21B37D
10	0X8D358C42	26	0X6EABD6DC	42	0X41D87AFD	58	0X3B770D63
11	0XE6ACE3DE	27	0X5071B039	43	0X7862292B	59	0X07BD5EC0
12	0X771A29C6	28	0X0CEFCEAB	44	0XCAC4B01F	60	0X50021570
13	0XAE63F75A	29	0XC51952F5	45	0X31AE8D69	61	0XF6F76806
14	0XBA63121F	30	0XC3946575	46	0X163F4C41	62	0XF5E9F3B6
15	0X73352CA3	31	0X09EE8B00	47	0X8FD9F79C	63	0X6C00345A

INDEX	VALUE
THE 1ST DATA FOR DISTURBING	0X1C71C71C71C7
THE 2ND DATA FOR DISTURBING	0X55555555